# อิทธิพลของจำนวนรอบในการตั้งรหัสผ่านกับการมีกฎในการเลือกรหัสผ่าน ต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ


โดย

นายธีรยุทธ เอกรุณ


วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2557

# อิทธิพลของจำนวนรอบในการตั้งรหัสผ่านกับการมีกฎในการเลือกรหัสผ่าน ต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ


โดย

นายธีรยุทธ เอกรุณ

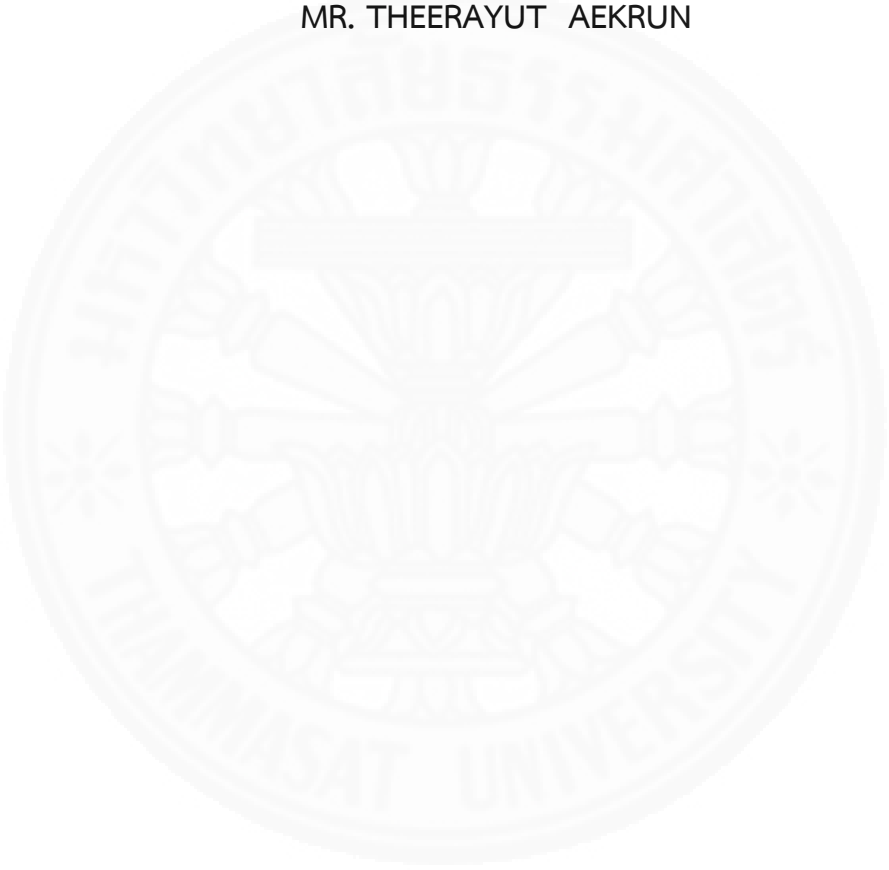


วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต
สาขาวิชาวิทยาการคอมพิวเตอร์ ภาควิชาวิทยาการคอมพิวเตอร์
คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์
ปีการศึกษา 2557

# THE INFLUENCE OF NUMBER OF PASSWORD SETTING TURNS AND RULES ON GRAPHICAL PASSWORD AUTHENTICATION

BY

MR. THEERAYUT AEKRUN



A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE
DEPARTMENT OF COMPUTER SCIENCE
FACULTY OF SCIENCE AND TECHNOLOGY
THAMMASAT UNIVERSITY
ACADEMIC YEAR 2014

มหาวิทยาลัยธรรมศาสตร์
คณะวิทยาศาสตร์และเทคโนโลยี

วิทยานิพนธ์

ของ

นายธีรยุทธ เอกรุณ

เรื่อง

อิทธิพลของจำนวนรอบในการตั้งรหัสผ่านกับการมีกฎในการเลือกรหัสผ่าน
ต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ

ได้รับการตรวจสอบและอนุมัติ ให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
วิทยาศาสตรมหาบัณฑิต

เมื่อ วันที่ 10 สิงหาคม พ.ศ. 2558

ประธานกรรมการสอบวิทยานิพนธ์ _____
(ดร.รัชต พีชวณิชย์)

กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ _____
(ผู้ช่วยศาสตราจารย์ ดร.ณัฐธนนท์ หงส์วริทธิ์ธร)

กรรมการสอบวิทยานิพนธ์ _____
(ผู้ช่วยศาสตราจารย์ ดร.เสาวลักษณ์ วรรธนาภา)

กรรมการสอบวิทยานิพนธ์ _____
(ดร.มารุต บูรณรัช)

คณบดี _____
(รองศาสตราจารย์ ปกรณ์ เสริมสุข)

| | |
|---|---|
| หัวข้อวิทยานิพนธ์ | อิทธิพลของจำนวนรอบในการตั้งรหัสผ่านกับการมีกฎในการเลือกรหัสผ่านต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ |
| ชื่อผู้เขียน | นายธีรยุทธ เอกรุณ |
| ชื่อปริญญา | วิทยาศาสตรมหาบัณฑิต |
| สาขาวิชา/คณะ/มหาวิทยาลัย | วิทยาการคอมพิวเตอร์<br>วิทยาศาสตร์และเทคโนโลยี<br>มหาวิทยาลัยธรรมศาสตร์ |
| อาจารย์ที่ปรึกษาวิทยานิพนธ์ | ผู้ช่วยศาสตราจารย์ ดร.ณัฐธนนท์ หงส์วริทธิ์ธร |
| ปีการศึกษา | 2557 |


## บทคัดย่อ


งานวิจัยนี้ทำการศึกษาถึงปัจจัยที่มีอิทธิพลต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยมีปัจจัยที่นำมาศึกษาเปรียบเทียบ 2 ปัจจัย ได้แก่ ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน ระหว่างการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ และปัจจัยการมีกฎในการเลือกรหัสผ่าน ระหว่างการมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มาใช้ในการออกแบบระบบการพิสูจน์ตัวตน เพื่อวิเคราะห์ถึงปัจจัยที่มีอิทธิพลต่อด้านการใช้งาน ด้านความปลอดภัย และความพึงพอใจของผู้ใช้งาน

งานวิจัยนี้เป็นการวิจัยเชิงทดลอง ใช้รูปแบบการทดลองแบบ 2x2 Between Subjects Design มีผู้เข้าร่วมการทดลองจำนวน 60 คน แบ่งออกเป็น 4 กลุ่มทดลอง โดยแต่ละกลุ่มได้ทำการทดลองกลุ่มละ 1 รูปแบบ เครื่องมือที่ใช้ในงานวิจัยได้พัฒนาโปรแกรมการพิสูจน์ตัวตนด้วยภาษา ASP.NET (C#.NET) ใช้ระบบจัดการฐานข้อมูล Microsoft SQL Server 2008 โดยมีแบบสอบถามข้อมูลทั่วไปและแบบสอบถามความพึงพอใจของผู้ใช้งาน การทดลองด้านการใช้งานและด้านความปลอดภัยทำการทดลองทั้งหมด 3 ครั้ง ได้แก่ ครั้งที่ 1 หลังจากการลงทะเบียนทันที ครั้งที่ 2 หลังจากการทะเบียนไปแล้ว 3 วัน และครั้งที่ 3 หลังจากการลงทะเบียนไปแล้ว 15 วัน โดยการวิเคราะห์ด้านการใช้งาน ประกอบด้วย จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน และการวิเคราะห์ด้านความปลอดภัย ประกอบด้วย จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน

ผลการทดลองด้านการใช้งานแสดงให้เห็นว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านมีอิทธิพลต่อการใช้งานอย่างมีนัยสำคัญทางสถิติ โดยการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่าและมีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่าการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ แต่ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่ส่งผลต่อด้านการใช้งาน เมื่อวิเคราะห์การมีอิทธิพลร่วมของทั้ง 2 ปัจจัย กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยที่สุด มีเวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตนน้อยที่สุด และมีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด ส่วนผลการทดลองด้านความปลอดภัย พบว่า การโจรกรรมรหัสผ่านด้วยวิธีการแอบมอง (Shoulder surfing) ไม่สามารถโจรกรรมการพิสูจน์ตัวตนได้สำเร็จทั้ง 4 กลุ่มทดลอง แต่ในแง่ของการคาดเดารหัสผ่านการไม่มีกฎในการเลือกรหัสผ่านรูปภาพจะมีความปลอดภัยมากกว่าการมีกฎในการเลือกรหัสผ่าน เนื่องจากมีความเป็นไปได้ของรหัสผ่านมากกว่าการมีกฎในการเลือกรหัสผ่าน ผลการวิเคราะห์ความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อโปรแกรมการพิสูจน์ตัวตนสามารถสรุปโดยรวมได้ว่าผู้เข้าร่วมการทดลองมีระดับความพึงพออยู่ในระดับพึงพอใจมาก

**คำสำคัญ:** การพิสูจน์ตัวตน, รหัสผ่านรูปภาพ, การโจรกรรมรหัสผ่านด้วยวิธีการแอบมอง

| | |
|---|---|
| Thesis Title | THE INFLUENCE OF NUMBER OF PASSWORD SETTING TURNS AND RULES ON GRAPHICAL PASSWORD AUTHENTICATION |
| Author | Mr. Theerayut Aekrun |
| Degree | Degree of Master of Science Program in Computer Science |
| Department/Faculty/University | Department of Computer Science<br>Faculty of Science and Technology<br>Thammasat University |
| Academic Years | 2014 |


## ABSTRACT


This research was to investigate two factors which affect on usability and security of identification process with graphical password. The two factors are a) number of cycles to set password, including one cycle and two cycle, and b) existing of rules for choose password, including existing of rules and no existing of rules. The 2x2 Between Subjects Design was employed. Experiment by group 60 court stuff in to 4 group follow factors that we want to experiment. We use ASP.NET (C#.NET) as a tool to construct program and use Microsoft SQL Server 2008 as a database. We process experiment by prepare general survey and satisfaction survey and request experiment group to complete general survey after finish they will need to identify and complete satisfaction survey. The experiments were tested three times for usability and security. The analysis of usability including the number is used to authentication, the average time spent on authentication and the success of the authentication. The analysis of security including the number is used in the theft of authentication, the average time spent in the theft of authentication and the success in the theft of authentication.

The experimental results show that the number of cycles to set password has an effect on usability but it does not effect on security. On the other hands, the existing of rules for choose password does not effect on usability and security. Use one cycle to set password and no existing of rules made users spend least time for

completing. Use one cycle to set password and no existing of rules to usability the best effect. Additionally, the users were satisfied with the created authentication program.

**Keywords:** Authentication, Graphical Password, Shoulder surfing

# กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี ด้วยความกรุณาจาก ดร.รัชต พีชวณิชย์ ประธานกรรมการสอบวิทยานิพนธ์ ผู้ช่วยศาสตราจารย์ ดร.เสาวลักษณ์ วรรธนาภา และดร.มารุต บูรณรัช กรรมการสอบวิทยานิพนธ์ ที่เสียสละเวลาในการเป็นกรรมการสอบและให้ข้อเสนอแนะในการปรับปรุงวิทยานิพนธ์ โดยเฉพาะอย่างยิ่งผู้ช่วยศาสตราจารย์ ดร.ณัฐธนนท์ หงส์วริทธิ์ธร กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่เสียสละเวลาให้ความอนุเคราะห์แนะนำแนวคิด แนวทางการทำงานวิจัย การแก้ไขปัญหาที่เกิดในงานวิจัยตลอดจนตรวจสอบข้อบกพร่องของงานวิจัย เพื่อให้วิทยานิพนธ์มีความถูกต้องและสมบูรณ์ กระผมรู้สึกซาบซึ้งในความกรุณาและขอกราบขอบพระคุณเป็นอย่างสูงมา ณ โอกาสนี้

ขอกราบขอบพระคุณคณาจารย์ทุกท่านที่มีส่วนในการประสิทธิ์ประสาทวิชาให้แก่ข้าพเจ้า และขอขอบพระคุณเจ้าหน้าที่ประจำภาควิชาวิทยาการคอมพิวเตอร์ทุกท่านที่ให้ความช่วยเหลือและอำนวยความสะดวกในทุกเรื่อง ตลอดระยะเวลาของการศึกษาและดำเนินการวิจัย

ขอขอบคุณข้าราชการศาลยุติธรรม และเจ้าหน้าที่ในศาลอุทธรณ์ภาค 7 ทุกท่าน ที่สละเวลาในการทำการทดลองของวิทยานิพนธ์ฉบับนี้

ขอขอบคุณนางสาวสุธินี ฤกษ์วศินกุล ที่คอยผลักดันและเป็นกำลังใจให้ข้าพเจ้าทำวิทยานิพนธ์ฉบับนี้ได้สำเร็จ นายเกรียงไกร มะโนใจ นายดนุพัฒน์ กชชาดาปภาดา นางสาวธัญลักษณ์ รามโกมุท ที่ให้คำปรึกษาในการพัฒนาโปรแกรมสำหรับการทดลอง นายภูริลาภ จุฑาวัชระพล นายภากร คูกรินทร์รัตน์ สำหรับการช่วยเหลือทางด้านวิชาการและภาษาอังกฤษที่ยอดเยี่ยม และขอขอบคุณเพื่อน ๆ CS@TU'54 ทุกคน ในมิตรภาพ ความห่วงใย และคำปรึกษาในด้านต่าง ๆ ท้ายที่สุดขอขอบพระคุณครอบครัวที่คอยสนับสนุนและเป็นกำลังใจ ตลอดมา

นายธีรยุทธ เอกรุณ

# สารบัญ

# สารบัญตาราง

# สารบัญภาพประกอบ

# บทที่ 1
# บทนำ

## 1.1 ความเป็นมาและความสำคัญของงานวิจัย

การพิสูจน์ตัวตน (Authentication) เป็นขั้นตอนการตรวจสอบสิทธิการเข้าถึงข้อมูลหรือการเข้าใช้ระบบต่าง ๆ อาทิเช่น การใช้คอมพิวเตอร์ส่วนบุคคล สมาร์ทโฟน แท็บเล็ต และระบบต่าง ๆ จดหมายอิเล็กทรอนิกส์ (E-mail) สังคมออนไลน์ (Social network) และระบบธุรกรรมทางการเงินที่ใช้งานผ่านระบบอิเล็กทรอนิกส์ เป็นต้น เพื่อการเก็บรักษาข้อมูลส่วนตัวและความปลอดภัยของข้อมูลในระบบเทคโนโลยีสารสนเทศจากผู้ไม่มีสิทธิหรือผู้ไม่หวังดี โดยการพิสูจน์ตัวตนสามารถจำแนกได้เป็น 3 ประเภท (Suo, Zhu, & Owen, 2005; Lashkari, 2010) ได้แก่ 1) การพิสูจน์ตัวตนโดยการใช้เอกลักษณ์เฉพาะบุคคล (Biometric based authentication หรือ Inherit based authentication) เช่น การสแกนลายนิ้วมือ การสแกนม่านตา หรือการจดจำใบหน้า ซึ่งเป็นวิธีที่มีความปลอดภัยสูงที่สุด แต่ยังไม่มีการนำมาใช้อย่างแพร่หลาย เนื่องจากต้องใช้อุปกรณ์ที่มีราคาแพงและกระบวนการทำงานที่ช้า 2) การพิสูจน์ตัวตนโดยการใช้อุปกรณ์โทเค่น (Token based authentication) เช่น คีย์การ์ด แบงค์การ์ด และสมาร์ทการ์ด มีการใช้งานอย่างแพร่หลาย โดยส่วนมากจะใช้ร่วมกับการพิสูจน์ตัวตนโดยใช้ฐานความรู้ เช่น บัตร ATM หรืออุปกรณ์ที่ใช้ร่วมกันหมายเลข PIN แต่วิธีการนี้จำเป็นต้องพกการ์ดต่าง ๆ และจำรหัสเพื่อใช้งาน ซึ่งหากลืมหรือเกิดสูญหายก็จะไม่สามารถทำการพิสูจน์ตัวตนได้ และวิธีนี้ค่อนข้างเสี่ยงต่อการถูกหลอกหลวงและถูกขโมย 3) การพิสูจน์ตัวตนโดยการใช้ฐานความรู้ (Knowledge based authentication) คือ การใช้ข้อมูลหรือความรู้ที่มีอยู่ของแต่ละบุคคลมากำหนดเป็นรหัสผ่าน โดยวิธีนี้จะร่วมทั้งการใช้รหัสผ่านตัวอักษร (Text-based passwords) และการใช้รหัสผ่านรูปภาพ (Picture-based passwords) ซึ่งการใช้รหัสผ่านรูปภาพจะสามารถแบ่งออกได้เป็น 2 ประเภท ได้แก่ 1) การรู้จำได้ (recognition-based) คือ การให้ผู้ใช้พิสูจน์ตัวตนด้วยการเลือกรูปภาพให้ถูกต้องตามที่ได้สร้างไว้ในขั้นตอนลงทะเบียน และ 2) การระลึกได้ (recall-based) คือ การให้ผู้ใช้พิสูจน์ตัวตนด้วยการสร้างรหัสผ่านรูปภาพอีกครั้งให้เหมือนกับที่เคยได้สร้างไว้ในขั้นตอนการลงทะเบียน

การพิสูจน์ตัวตนที่เป็นที่นิยมและมีการใช้งานอย่างแพร่หลาย คือ การพิสูจน์ตัวตนด้วยรหัสผ่านตัวอักษร โดยการใช้ตัวอักษรแทนบัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเป็นการยืนยันถึงการมีสิทธิเข้าถึงข้อมูลหรือเข้าใช้ระบบงาน แต่การใช้การพิสูจน์ตัวตนด้วยรหัสผ่านตัวอักษรก็ยังมีปัญหาในด้านการจดจำ โดยเฉพาะในกรณีที่ต้องการให้รหัสผ่านตัวอักษรมีความ

ปลอดภัย ก็จะต้องตั้งรหัสผ่านตามหลักเกณฑ์ต่าง ๆ เช่น รหัสผ่านต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยประกอบไปด้วยตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และอักขระพิเศษ เช่น @ # $ % เป็นต้น และไม่ใช้ข้อมูลส่วนตัวในการตั้งรหัสผ่าน เช่น ชื่อของผู้ใช้ ชื่อเล่นหรือฉายา เบอร์โทรศัพท์ หรือชื่อบริษัท เป็นต้น และไม่ใช้คำที่มีในพจนานุกรมหรือคำที่มีความหมาย ซึ่งการตั้งรหัสผ่านตามหลักเกณฑ์ข้างต้นมีความปลอดภัยสูงก็จริง แต่เป็นปัญหาต่อผู้ใช้งานในด้านการจดจำรหัสผ่าน ผู้ใช้ส่วนมากจึงต้องจดบันทึกรหัสผ่าน (Kotadia, 2005, p. 594-597) หรือสร้างรหัสผ่านให้เหมือนกันทุกบัญชี (Dhamija & Perrig, 2000) เพื่อให้สามารถจดจำรหัสผ่านได้ง่าย แต่ทำให้รหัสผ่านมีโอกาสถูกโจรกรรมได้ง่ายและเกิดความไม่ปลอดภัยในบัญชีที่มีการตั้งรหัสผ่านเหมือนกัน และในกรณีที่ผู้ใช้ต้องการตั้งรหัสผ่านให้สามารถจดจำได้ง่าย โดยเลือกการตั้งรหัสผ่านที่สั้นและง่าย (Adams & Sasse, 1999, pp. 41-46) เช่น การใช้ข้อมูลส่วนตัวในการตั้งรหัสผ่าน ได้แก่ วัน เดือน ปีเกิด เบอร์โทรศัพท์ ชื่อบุคคลในครอบครัว เป็นต้น (คณิน อุดมสุขประเสริฐ, 2555) ก็จะทำให้รหัสผ่านนั้นมีความปลอดภัยต่ำ สามารถคาดเดาได้ง่าย ซึ่งอาจถูกผู้ไม่หวังดีที่เชี่ยวชาญด้านคอมพิวเตอร์ (Cracker) ทำการโจรกรรมรหัสผ่านของระบบพิสูจน์ตัวตนได้ด้วยวิธีการต่าง ๆ เช่น การสุ่มรหัสผ่านในทุกความเป็นไปได้ของตัวอักษร (Brute force attack) การสุ่มรหัสผ่านโดยใช้คำในพจนานุกรม (Dictionary attack) ซอฟต์แวร์สอดแนม (Spyware attack) การใช้วิธีการแอบมอง (Shoulder surfing attack) และการใช้วิธีการหาข้อมูลจากสิ่งรอบตัวของผู้ใช้ (Social engineering attack) เป็นต้น

จากปัญหาความสามารถในการจดจำรหัสผ่านตัวอักษรของผู้ใช้ จึงได้มีงานวิจัยเกี่ยวกับการนำรูปภาพมาใช้ในการพิสูจน์ตัวตน โดยอ้างอิงจากผลการวิจัยว่า มนุษย์สามารถจดจำและระลึกรูปภาพได้ดีกว่าตัวอักษร (Shepard, 1967; Paivio, Rogers, & Smythe, 1968, pp. 137-138) โดยงานวิจัยที่นำรูปภาพมาใช้ในการพิสูจน์ตัวตนที่ผู้วิจัยได้ศึกษาและสนใจคือ การพิสูจน์ตัวตนด้วยวิธีการที่เรียกว่า Passface (RealUser, 2005) โดยผู้ใช้จะต้องทำการเลือกรูปภาพใบหน้าคนจำนวน 4 ภาพ เพื่อใช้เป็นรหัสผ่าน ในขั้นตอนการพิสูจน์ตัวตน ระบบจะแสดงรูปภาพใบหน้าคนในตารางกริดจำนวนทั้งหมด 9 ภาพ โดยจะมีรูปภาพ 1 ภาพ เป็นภาพที่ผู้ใช้ได้ทำการเลือกไว้ และอีก 8 ภาพ เป็นภาพหลอก โดยผู้ใช้จะต้องทำการเลือกภาพที่ได้ทำการเลือกไว้ในขั้นตอนการสร้างรหัสผ่าน จนครบ 4 ภาพ แต่เนื่องจากวิธีการนี้ใช้เมาส์ในการเลือกรหัสผ่าน จึงทำให้การโจมตีจากการแอบมอง (Shoulder Surfing Attack) สามารถโจรกรรมรหัสผ่านได้ และได้มีงานวิจัยการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่เรียกว่า Secure Passface หรือ S-Passface (Farnaz, Maslin, & Azizah, 2013, pp. 135-141) ที่นำเอา Passface มาพัฒนาเพื่อปรับปรุง ด้านความปลอดภัย ในการป้องกันการโจมตีจากการแอบมอง (Shoulder surfing attack) โดยใช้วิธีการเลือกรหัสผ่านด้วยการใช้คีย์บอร์ดพิมพ์ตัวอักษรใต้รูปภาพที่ต้องการเลือก แทนการใช้เมาส์ ซึ่งจากผลการทดลองด้านความปลอดภัย สามารถป้องกันการโจมตีจากการแอบมอง (Shoulder surfing attack) ได้ถึง 100 เปอร์เซ็นต์ แต่ผลการทดลองด้าน

การใช้งานพบว่าความง่ายในการใช้งานลดลง เมื่อเทียบกับ Passface จึงเป็นเรื่องที่น่าสนใจหากนำเอารูปแบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบ S-Passface มาประยุกต์ใช้ในการออกแบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพเพื่อเพิ่มความง่ายในการใช้งาน และยังคงความปลอดภัยไว้ด้วย

จากความสำคัญของปัญหาการพิสูจน์ตัวตนและงานวิจัยดังกล่าวข้างต้น ผู้วิจัยเห็นว่าเพื่อประโยชน์ของผู้ใช้งานในการเก็บรักษาข้อมูลที่สำคัญในระบบเทคโนโลยีสารสนเทศ และเพื่อวิเคราะห์หารูปแบบในการออกแบบและพัฒนา วิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่สามารถใช้งานง่าย (Usability) และมีความปลอดภัย (Security) ผู้วิจัยจึงนำเอารูปแบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่มีลักษณะเดียวกับ S-Passface มาประยุกต์ใช้เพื่อการศึกษาถึงปัจจัยที่มีอิทธิพลต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยมีปัจจัยที่นำมาศึกษาเปรียบเทียบ 2 ปัจจัย ได้แก่ ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน ระหว่างการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ และปัจจัยการมีกฎในการเลือกรหัสผ่าน ระหว่างการมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มาใช้ในการออกแบบระบบการพิสูจน์ตัวตน เพื่อวิเคราะห์ถึงปัจจัยที่มีอิทธิพลต่อด้านการใช้งาน ด้านความปลอดภัย และความพึงพอใจของผู้ใช้งาน

## 1.2 ปัญหานำวิจัย

งานวิจัยนี้ทำการศึกษาเปรียบเทียบปัจจัยที่มีอิทธิพลต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยมีปัจจัยที่นำมาศึกษาเปรียบเทียบ 2 ปัจจัย ได้แก่ ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน ระหว่างการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ และปัจจัยการมีกฎในการเลือกรหัสผ่าน ระหว่างการมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท เพื่อวิเคราะห์ถึงปัจจัยที่มีอิทธิพลต่อด้านการใช้งาน ด้านความปลอดภัย และความพึงพอใจของผู้ใช้งาน

## 1.3 วัตถุประสงค์งานวิจัย

1. เพื่อเปรียบเทียบด้านการใช้งาน (Usability) ด้านความปลอดภัย (Security) และความพึงพอใจของผู้ใช้ที่มีต่อการพิสูจน์ตัวตน ระหว่างการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ

2. เพื่อเปรียบเทียบด้านการใช้งาน (Usability) ด้านความปลอดภัย (Security) และความพึงพอใจของผู้ใช้ที่มีต่อการพิสูจน์ตัวตน ระหว่างการมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

3. เพื่อศึกษาปัจจัยที่มีอิทธิพลร่วมกันในด้านการใช้งาน (Usability) ด้านความปลอดภัย (Security) และความพึงพอใจของผู้ใช้ที่มีต่อการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่าน กับปัจจัยการมีกฎในการเลือกรหัสผ่าน

4. เพื่อเปรียบเทียบด้านการใช้งาน (Usability) ด้านความปลอดภัย (Security) และความพึงพอใจของผู้ใช้ที่มีต่อการพิสูจน์ตัวตน กับรูปแบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่มีลักษณะเดียวกับ S-Passface

**1.4 ขอบเขตงานวิจัย**

เพื่อให้งานวิจัยบรรลุถึงวัตถุประสงค์ จึงได้กำหนดขอบเขตของการวิจัยไว้ดังต่อไปนี้

1. กลุ่มตัวอย่างที่ใช้ในการวิจัยครั้งนี้ เป็นเจ้าหน้าที่ในศาลอุทธรณ์ภาค 7 โดยมุ่งเน้นศึกษาเฉพาะกลุ่มตัวอย่าง ที่เคยใช้งานระบบพิสูจน์ตัวตนและใช้งานคอมพิวเตอร์มาแล้วอย่างน้อย 1 ปี ทั้งเพศชาย และเพศหญิง จำนวนทั้งหมด 60 คน โดยได้แบ่งออกเป็น 4 กลุ่มทดลอง กลุ่มทดลองละ 15 คน

2. การทดลองด้านการใช้งาน (Usability) จะทำการทดลองการพิสูจน์ตัวตนทั้งหมด 3 ครั้ง ได้แก่ ครั้งที่ 1 หลังจากการลงทะเบียนทันที ครั้งที่ 2 หลังจากการลงทะเบียนไปแล้ว 3 วัน และครั้งที่ 3 หลังจากการลงทะเบียนไปแล้ว 15 วัน

3. การทดลองด้านความปลอดภัย (Security) จะทำการทดลองการโจรกรรมรหัสผ่านโดยวิธีการแอบมอง (Shoulder surfing) ทั้งหมด 3 ครั้ง ได้แก่ หลังจากที่ผู้เข้าร่วมการทดลองทำการทดลองด้านการใช้งานเสร็จสิ้นทั้ง 3 ครั้ง

4. การประเมินประสิทธิภาพของวิธีการพิสูจน์ตัวตนที่ออกแบบนี้ โดยการวัดประสิทธิภาพด้านการใช้งานซึ่งประกอบไปด้วย จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน สำหรับการวัดประสิทธิภาพด้านความปลอดภัยจะประกอบไปด้วย จำนวนครั้งที่ใช้ในการโจรกรรมพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมพิสูจน์ตัวตน อีกทั้งได้ทำการวัดความพึงพอใจผู้ใช้ที่มีต่อระบบพิสูจน์ตัวตนด้วยแบบสอบถามความพึงพอใจ ขั้นตอนสุดท้ายจะนำข้อมูลที่ได้จากการทดลองเหล่านี้มาเปรียบเทียบตามปัจจัยที่ศึกษาเพื่อวิเคราะห์ผลการวิจัยว่ามีความแตกต่างกันอย่างไร

## 1.5 ประโยชน์ที่คาดว่าจะได้รับ

จากการดำเนินการวิจัยตามวัตถุประสงค์ และขอบเขตการวิจัยที่กำหนดไว้ ผู้วิจัยคาดว่าจะได้รับประโยชน์จากงานวิจัย ดังต่อไปนี้

1. เพื่อทราบถึงความแตกต่างของวิธีการพิสูจน์ตัวตน แบบมีปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน ในด้านการใช้งาน (Usability) ด้านความปลอดภัย (Security) และความพึงพอใจ

2. เพื่อทราบถึงรูปแบบในการออกแบบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่เหมาะสม ให้มีการใช้งานที่ง่าย (Usability) และมีความปลอดภัยสูง (Security)

3. เพื่อนำข้อมูลจากการศึกษาวิจัยครั้งนี้เป็นพื้นฐานในการศึกษาวิจัยที่เกี่ยวข้องต่อไป หรือเป็นแนวทางในการประยุกต์ใช้กับงานวิจัยด้านอื่นที่เกี่ยวข้องกับการออกแบบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ

## 1.6 รายละเอียดงานวิจัย

รายละเอียดของวิทยานิพนธ์ฉบับนี้ แบ่งออกเป็น 5 บท ดังนี้

บทที่ 1 บทนำ ประกอบด้วย ความเป็นมาและความสำคัญของงานวิจัย ปัญหานำวิจัย วัตถุประสงค์งานวิจัย สมมติฐาน ขอบเขตงานวิจัย ประโยชน์ที่คาดว่าจะได้รับ และรายละเอียดงานวิจัย

บทที่ 2 ทฤษฎีและงานวิจัยที่เกี่ยวข้อง ประกอบด้วย ทฤษฎีที่เกี่ยวกับความจำของมนุษย์ การใช้รูปแบบอักษร และงานวิจัยที่เกี่ยวข้องกับการออกแบบระบบพิสูจน์ตัวตน

บทที่ 3 วิธีการดำเนินงานวิจัย ประกอบด้วย ระเบียบวิธีการทดลอง โครงสร้างและขั้นตอนการทำงานของระบบ การออกแบบการทดลอง และการวัดผลการทดลอง

บทที่ 4 ผลการทดลอง ประกอบด้วย ผลการทดลองด้านประสิทธิภาพการใช้งาน ผลการทดลองด้านประสิทธิภาพความปลอดภัย ผลคะแนนความพึงพอใจ และผลการวิเคราะห์โปรแกรมที่ออกแบบ

บทที่ 5 สรุปผลการวิจัยและข้อเสนอแนะ ประกอบไปด้วย สรุปผลที่ได้จากการวิจัย การอภิปรายผลและข้อเสนอแนะ และแนวทางการศึกษาวิจัยต่อไปในอนาคต

ในส่วนของบทต่อไปนั้น จะกล่าวถึงทฤษฎีและงานวิจัยที่เกี่ยวข้อง ที่ได้ศึกษาและนำมาเป็นแนวทางในการทำงานวิจัยนี้

# บทที่ 2
# ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

ในบทนี้จะนำเสนอทฤษฎีที่เกี่ยวกับความจำของมนุษย์ และงานวิจัยด้านการพิสูจน์ตันตนโดยการใช้รูปภาพที่ผ่านมา เพื่อเป็นแนวทางในการวิจัยและการออกแบบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยมีรายละเอียดดังนี้

## 2.1 ทฤษฎีที่เกี่ยวข้อง

งานวิจัยนี้มีการศึกษาด้านการใช้งานของการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยมีการวัดผลการใช้งานที่เกี่ยวข้องกับการจดจำ ผู้วิจัยจึงขอกล่าวถึงทฤษฎีที่เกี่ยวกับความจำของมนุษย์ที่ได้ศึกษาจากหนังสือความจำมนุษย์ (อุบลรัตน์ เพ็งสถิตย์, 2535)โดยมีรายละเอียดดังต่อไปนี้

### 2.1.1 ความหมายของความจำ

ความจำ หมายถึง กระบวนการอย่างหนึ่งทางจิตใจ ซึ่งเป็นกระบวนการที่จะเป็นความสามารถในการตอบสนองต่อบางสิ่งบางอย่างที่เคยมีประสบการณ์มาแล้ว ให้สามารถแสดงออกมาได้อีกครั้งหนึ่ง หรืออาจกล่าวได้ง่าย ๆ ว่าเป็นความสามารถในการระลึกถึงเหตุการณ์หรือสิ่งต่าง ๆ ให้ฟื้นกลับมาอีกครั้งหนึ่ง

### 2.1.2 ประเภทของความจำ

การพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพผู้ใช้จำเป็นต้องอาศัยความจำเพื่อให้สามารถนำรหัสผ่านที่ได้สร้างมาใช้ในการพิสูจน์ตัวตนเมื่อต้องการใช้งานข้อมูลหรือระบบต่าง ๆ โดยความจำสามารถแบ่งออกได้เป็น 2 ประเภท ได้แก่

(1) ความจำระยะสั้น (Short – Term Memory) มีชื่อย่อว่า STM เป็นความจำที่เกิดขึ้นภายหลังจากการเกิดเหตุการณ์ต่าง ๆ เป็นความจำหลังการเรียนรู้ เมื่อเกิดความจำระยะสั้นแล้วจะปรากฏว่าความจำนั้นสามารถเลือนหายไปในระยะเวลาที่รวดเร็วมาก ความจำระยะสั้นจัดเป็นความจำชั่วคราว เกิดขึ้นมาเพื่อใช้ประโยชน์ในขณะที่จำอยู่เท่านั้น เช่น จำหมายเลขโทรศัพท์ เมื่อ กดหมายเลขโทรศัพท์เสร็จสิ้นแล้ว และกำลังพูดโทรศัพท์อยู่นั้น ปรากฏว่าลืมหมายเลขโทรศัพท์นั้นทันที ดังนั้น ความจำระยะสั้นจัดว่าเป็นความจำที่จะสูญหายไปอย่างง่ายดาย ถ้าหากว่าเราไม่ได้ตั้งใจหรือใส่ใจที่จะจดจำ

(2) ความจำระยะยาว (Long – Term Memory) มีชื่อย่อว่า LTM เป็นเหตุการณ์ที่เกิดขึ้นและสามารถจะจำได้ภายในนาที หรืออาจจะเป็นวัน สัปดาห์ ปี หรือหลาย ๆ ปีก็

เป็นได้ เมื่อมีการระลึกถึงสิ่งนั้น ๆ จะสามารถระลึกได้ทันที ความจำระยะยาวนี้จะต้องมีกระบวนการที่ผ่านกระบวนการของความจำระยะสั้นมาก่อนเสมอ การที่บุคคลสามารถจดจำสิ่งต่าง ๆ ได้ดีมากน้อยเท่าใดนั้น ขึ้นอยู่กับกระบวนการที่เราจะมีความสามารถในการบรรจุความจำส่วนนั้น ๆ เข้าสู่ความจำระยะยาวได้ดีมากน้อยเพียงใด ปัญหาที่สำคัญสำหรับการบรรจุความจำลงในสมองนั้น คือ บุคคลมักจะถูกแทรกแซงด้วยสิ่งต่าง ๆ ตามหลักการของ Interference Theory เช่น “ฉันไม่สามารถนึกถึงชื่อครูที่เคยสอนชั้นประถมปีที่ 4 ได้ เพราะชื่อครูที่สอนในชั้นประถมปีที่ 3 มาคอยรบกวนฉันตลอดเวลา” หลักการแทรกแซงที่ทำให้ความจำระยะยาวเกิดขึ้นไม่ได้ มีหลัก 2 ประการดังนี้

1. กิจกรรมที่ทำให้การเรียนรู้ใหม่เกิดขึ้นไม่ได้ เพราะ การเรียนรู้เดิมหรือกิจกรรมเดิมรบกวนทำให้การเรียนรู้สิ่งใหม่ไม่ได้ผลดี หรือบางครั้งการเรียนรู้สิ่งใหม่อาจจะไม่เกิดขึ้นเลยก็ได้ เรียกว่า การแทรกแซงตาม

2. กิจกรรมที่ทำให้เกิดการลืมเลือนในสิ่งที่ได้เรียนรู้ไป นั้นคือ การเรียนรู้สิ่งใหม่จะสามารถทำได้ดี และสิ่งที่ได้เรียนรู้มาแล้วในอดีตเกิดการลืมเลือน ทำให้จดจำกิจกรรมเดิมไม่ได้ เรียกว่า การแทรกแซงย้อนกลับ

ดังนั้น เพื่อให้ผู้เข้าร่วมการทดลองมีความตั้งใจหรือใส่ใจที่จะจดจำรหัสผ่านนำไปสู่การเกิดความจำระยะยาว เพื่อให้สามารถระลึกรหัสผ่านในการพิสูจน์ตัวตนได้นั้น ในการออกแบบการทดลองจำเป็นต้องหาวิธีการที่ให้ผู้เข้าร่วมการทดลองมีความตั้งใจหรือใส่ใจในการจดจำรหัสผ่านเพื่อให้ได้ผลการทดลองที่ถูกต้องและน่าเชื่อถือ

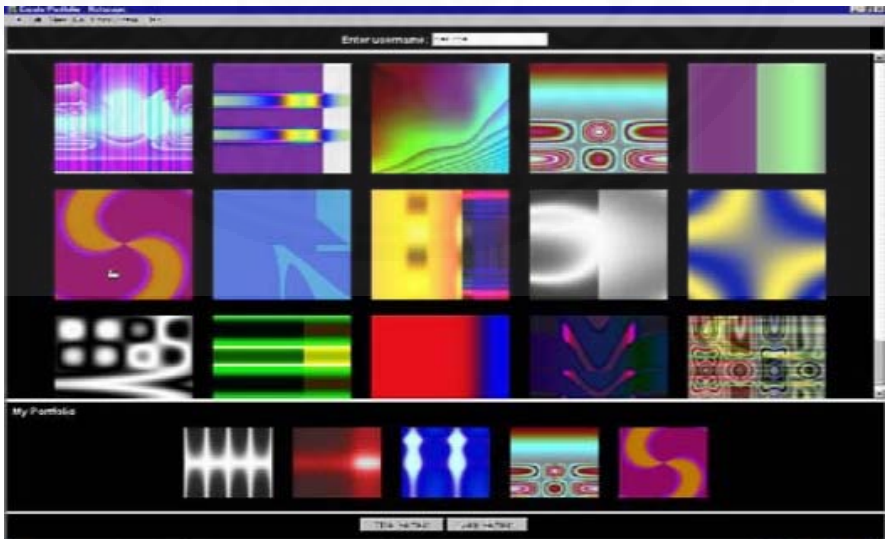
## 2.2 งานวิจัยที่เกี่ยวข้อง

คณิน อุดมสุขประเสริฐ (2555) ได้ศึกษาพฤติกรรมการตั้งรหัสผ่านของผู้ใช้งานอินเทอร์เน็ตวัยทำงานในประเทศไทย เก็บข้อมูลจากกลุ่มตัวอย่างจำนวน 494 คน พบว่ามีพฤติกรรมการตั้งรหัสผ่านโดยใช้ข้อมูลที่เกี่ยวข้องกับตนเอง จำนวน 395 คน คิดเป็นร้อยละ 80 และประชากรที่ไม่เคยใช้รหัสผ่านจากข้อมูลที่เกี่ยวข้องกับตนเองมีจำนวน 99 คน คิดเป็นร้อยละ 20 และข้อมูลที่เกี่ยวข้องกับตนเองที่นิยมใช้กำหนดเป็นรหัสผ่านเป็นอันดับแรกคือ วัน เดือน ปีเกิด มีจำนวน 148 คน คิดเป็นร้อยละ 30.0 ใช้เบอร์โทรศัพท์กำหนดเป็นรหัสผ่านจำนวน 81 คน คิดเป็นร้อยละ 16.4 ใช้ชื่อหรือฉายาของตนเองกำหนดเป็นรหัสผ่านจำนวน 86 คน คิดเป็นร้อยละ 17.4 ใช้ชื่อของบุคคลอื่นกำหนดเป็นรหัสผ่านจำนวน 32 คน คิดเป็นร้อยละ 6.5 ใช้ชื่อสัตว์เลี้ยงกำหนดเป็นรหัสผ่านจำนวน 12 คน คิดเป็นร้อยละ 2.4 ใช้เลขประจำตัวประชาชนหรือนักศึกษาจำนวน 21 คน คิดเป็นร้อยละ 4.3 ใช้ทะเบียนรถหรือเลขที่บ้านกำหนดเป็นรหัสผ่านจำนวน 4 คน คิดเป็นร้อยละ 0.8 ใช้วันสำคัญของคนในครอบครัวจำนวน 3 คน คิดเป็นร้อยละ 0.6 ใช้ข้อมูลส่วนตัวต่าง ๆ จำนวน 17 คน คิดเป็นร้อย

ละ 3.4 ใช้ชื่อสิ่งของหรือของใช้ส่วนตัวจำนวน 23 คน คิดเป็นร้อยละ 4.7 ใช้การสุ่มต่าง ๆ จำนวน 41 คน คิดเป็นร้อยละ 8.3 ใช้กลุ่มตัวเลขจำนวน 4 คน คิดเป็นร้อยละ 0.8 และไม่ระบุข้อมูลที่ใช้จำนวน 22 คน คิดเป็นร้อยละ 4.5

Tari, Ozok, & Holden (2006) ได้ทำการทดลองเปรียบเทียบการโจรกรรมรหัสผ่านด้วยวิธีการ Shoulder surfing กับระบบการพิสูจน์ตันตน 4 แบบ ได้แก่ รหัสผ่านตัวอักษรที่มีใน Dictionary รหัสผ่านตัวอักษรที่ไม่มีใน Dictionary รหัสผ่าน Passface แบบใช้เมาส์คลิกเลือก และรหัสผ่าน Passface แบบใช้คีย์บอร์ดเลือก โดยใช้ผู้ทดสอบทั้งหมด 20 คน ซึ่งผลที่ได้จากการทดลองพบว่า รหัสผ่าน Passface แบบใช้เมาส์คลิกเลือกนั้น จะโดนโจรกรรมรหัสผ่านด้วยวิธีการ Shoulder surfing มากที่สุด ซึ่งตรงกับแนวคิดของผู้เข้าร่วมการทดลองทั้ง 20 คน ซึ่งแสดงให้เห็นว่ารหัสผ่านรูปภาพมีจุดอ่อนในเรื่องของการโดนโจมตีด้วยวิธีการ Shoulder surfing ได้ง่าย

Akula and Devisetty (2004) ได้ออกแบบ Algorithm โดยระบบจะแสดงชุดของภาพและให้ผู้ใช้งานเลือกภาพรหัสผ่านให้ถูกต้อง ซึ่งมีวิธีการที่คล้ายกับวิธี “Déjà vu” (Dhamija & Perrig, 2000) แต่แตกต่างกันคือ Hash Function ที่ใช้จะเป็น SHA-1 โดยจะทำให้วิธีการพิสูจน์ตัวตนแบบดังกล่าวมีความปลอดภัยขึ้นและใช้หน่วยความจำน้อยลง แต่ไฟล์ภาพยังคงใช้พื้นที่มากกว่าการเก็บข้อมูลเป็นตัวอักขระถึงแม้จะผ่านวิธีการ Hash Function แล้วก็ตาม ผู้ทดลองชี้ให้เห็นว่าหากทำการปรับปรุงเรื่องการจัดเก็บข้อมูลให้ดีขึ้น ในอนาคตอาจจะนำมาปรับใช้กับโทรศัพท์มือถือและพีดีเอ (PDA) ได้



*ภาพที่ 2.1* Déjà vu by R. Dhamija, and A. Perrig, 2000, *A User Study Using Images for Authentication*, Proceedings of 9th USENIX Security Symposium.

RealUser Corporation 2005 ได้ทำการพัฒนาวิธีการที่เรียกว่า “Passface” ผู้ใช้จะต้องทำการเลือกภาพหน้าคนจำนวน 4 ภาพ เพื่อใช้เป็นรหัสผ่าน ในขั้นตอนการพิสูจน์ตัวตน ระบบจะแสดงภาพหน้าคนในตารางกริดจำนวนทั้งหมด 9 ภาพ โดยหนึ่งในนั้นจะมีรูปภาพ 1 ภาพเป็นภาพที่ผู้ใช้ได้ทำการเลือกไว้เป็นรหัสผ่านและอีก 8 ภาพที่เป็นภาพหลอก โดยผู้ใช้จะต้องทำการเลือกภาพที่ได้ทำการเลือกไว้ในขั้นตอนการสร้างรหัสผ่าน โดยขั้นตอนดังกล่าวจะต้องทำซ้ำจนครบ 4 ครั้งและเลือกภาพที่ถูกต้องครบทั้ง 4 ภาพ

โดย “Passface” ได้ทำการพัฒนาขึ้นภายใต้สมมุติฐานที่ว่ามนุษย์สามารถที่จะจดจำและระลึกถึงใบหน้ามนุษย์ด้วยกันได้ดีกว่ารูปภาพ ซึ่งมีงานวิจัยที่แสดงให้เห็นว่า “Passface” สามารถจดจำได้ง่ายในช่วงเวลาที่ยาวนาน (Valentine 1998, 1999) แต่อย่างไรก็ตามการพิสูจน์ตัวตนด้วยวิธีการดังกล่าวมีความล้มเหลว 1 ใน 3 เมื่อเปรียบเทียบกับการพิสูจน์ตัวตนด้วยรหัสผ่านตัวอักขระเนื่องจากใบหน้าที่ได้นำมาทำการทดลองอาจจะไม่เป็นที่รู้จักของผู้เข้าร่วมการทดลอง ซึ่งจะเป็นเรืองยากในการจดจำหรือวิเคราะห์ภาพดังกล่าว (Brostoff & Sasse, 2000)

*ภาพที่ 2.2* Passface by RealUser Corporation, 2005, from http://www.realuser.com

Towhidi, Masrom, & Manaf (2013) ได้เสนอวิธีการที่เรียกว่า “S-Passface” โดยได้มีการปรับปรุงความปลอดภัยของงานวิจัย “Passface” เพื่อป้องกันการโจมตีจากการแอบมอง (Shoulder Surfing Attack) โดยการทดลองจะให้ผู้เข้าร่วมการทดลองจะต้องทำการสร้างรหัสผ่านสองรอบ โดยรอบแรกจะให้ผู้เข้าร่วมการทดลองเลือกภาพใบหน้าคนจำนวนทั้งหมด 4 ภาพ ที่แสดงบนตารางกริดขนาด 3x3 สองตาราง โดยทำการเลือกตารางละ 2 ภาพ โดยตารางแรกระบบจะแสดง

ภาพใบหน้าผู้ชายและตารางที่สองจะแสดงภาพใบหน้าผู้หญิง ซึ่งจะมีตัวอักขระภาษาอังกฤษกำกับใต้ภาพทุกภาพซึ่งจะไม่ซ้ำกันในแต่ละภาพ โดยผู้เข้าร่วมการทดลองจะต้องนำตัวอักขระที่ปรากฏใต้ภาพไปกรอกยังช่องสำหรับรหัสผ่านแทนการเลือกรูปภาพ รอบที่สองระบบจะแสดงภาพหน้าคนให้ผู้เข้าร่วมการทดลองเลือกเหมือนรอบแรกแต่ภาพที่ใช้จะเป็นภาพของใบหน้าเด็กและตัวตลก ดังภาพที่ 2.7 หลังจากที่ได้ทำการเลือกภาพรหัสผ่านครบทั้งสองรอบแล้วจะให้ผู้เข้าร่วมการทดลองพิสูจน์ตัวตน ผลการทดลองพบว่าผู้ที่ทำการโจมตีรหัสผ่านไม่สามารถที่จะโจมตีรหัสผ่านได้ครบทั้ง 4 ภาพ ประมาณร้อยละ 8 ทำการเลือกภาพที่ถูกต้องได้สามภาพ ร้อยละ 25 ทำการเลือกภาพที่ถูกต้องได้สองภาพ ร้อยละ 35 ทำการเลือกภาพที่ถูกต้องได้หนึ่งภาพและร้อยละ 33 ของผู้ที่ทำการโจมตีรหัสผ่านทั้งหมด เลือกภาพไม่ถูกต้องเลย เมื่อเปรียบเทียบกับ Passface พบว่าร้อยละ 53 ของผู้โจมตีสามารถโจมตีรหัสผ่านได้ทั้งหมดและผู้โจมตีทุกคนสามารถโจมตีรหัสผ่านได้อย่างน้อยหนึ่งรูปภาพ ซึ่งแสดงให้เห็นว่า S-Passface สามารถป้องกันการโจมตีแบบการแอบมอง (Shoulder Surfing Attack) ได้ถึง 100 เปอร์เซ็นต์ แต่วิธีการนี้จะทำให้ความใช้งานง่ายลดลงเช่นกัน


*ภาพที่ 2.3* S-Passface by T. Farnaz, M. Maslin, and A.M. Azizah, 2013, *An Enhancement on Passface Graphical Password Authentication,* Vol. 3(2), p. 135-141. Journal of Basic and Applied Scientific Research.

จากการศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้อง จะเห็นได้ว่าการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพนั้น ช่วยให้ผู้ใช้งานสามารถจดจำรหัสผ่าน และเพิ่มโอกาสในการพิสูจน์ตัวตนสำเร็จมากกว่าการพิสูจน์ตัวตนด้วยรหัสตัวอักษร และการใช้คีย์บอร์ดในการเลือกใส่รหัสผ่านรูปภาพจะมีความปลอดภัยจากการถูกโจรกรรมด้วยวิธีการ Shoulder surfing มากกว่าการใช้เมาส์ โดยวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบ S-Passface นั้น ได้นำเอาข้อดีของการใช้รูปภาพใบหน้าคนเป็นรหัสผ่าน ที่สามารถเพิ่มความสามารถในการจดจำได้ดีกว่ารหัสผ่านแบบตัวอักษร อีกทั้งการใช้คีย์บอร์ดในการใส่รหัสผ่านที่มีความปลอดภัยมากกว่าการใช้เมาส์มาใช้ในการออกแบบทำให้มีความ

ปลอดภัยจากการโจรกรรมด้วยวิธีการ Shoulder surfing ถึง 100 เปอร์เซ็นต์ แต่อย่างไรก็ตาม การให้ผู้ใช้เลือกรูปภาพจากประเภทของรูปภาพที่ผู้ใช้ไม่มีความสนใจหรือไม่สามารถหาจุดเด่นของรูปภาพในประเภทนั้นได้ ก็อาจจะส่งผลต่อการใช้งานและความสามารถในการจดจำ และการที่ต้องใช้จำนวนรอบในการลงทะเบียนและการพิสูจน์ตันตนถึง 2 รอบ อาจทำให้ผู้ใช้งานเกิดความสับสน และต้องใช้เวลาในการลงทะเบียนและการพิสูจน์ตันตนมาก ก็อาจจะส่งผลกระทบต่อการใช้งานได้เช่นกัน ดังนั้น ผู้วิจัยจึงนำเอารูปแบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่มีลักษณะแบบ S-Passface มาประยุกต์ใช้เพื่อการศึกษาถึงปัจจัยที่มีอิทธิพลต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยมีปัจจัยที่นำมาศึกษาเปรียบเทียบ 2 ปัจจัย ได้แก่ จำนวนรอบในการตั้งรหัสผ่าน ระหว่างการใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ และการใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ และปัจจัยการมีกฎในการเลือกรหัสผ่าน ระหว่างการมีกฎในการเลือกรหัสผ่านประเภทละ 2 รูปภาพ และการไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท เพื่อวิเคราะห์ถึงปัจจัยที่มีอิทธิพลต่อด้านการใช้งาน (Usability) ด้านความปลอดภัย (Security) และความพึงพอใจของผู้ใช้งาน

# บทที่ 3
# วิธีดำเนินงานวิจัย

งานวิจัยนี้ทำการศึกษาเปรียบเทียบปัจจัยที่มีอิทธิพลต่อวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยปัจจัยที่นำมาศึกษาเปรียบเทียบ ได้แก่ ปัจจัยจำนวนรอบในการตั้งรหัสผ่านรูปภาพและปัจจัยการมีกฎในการลือกรหัสผ่านรูปภาพ เพื่อหารูปแบบวิธีการพิสูจน์ตัวตนที่มีการใช้งานที่ง่าย (Usability) และมีความปลอดภัยสูง (Security) โดยนำเอารูปแบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่มีลักษณะแบบเดียวกับ S-Passface มาประยุกต์ใช้ในการออกแบบ โดยในบทนี้จะนำเสนอระเบียบวิธีการทดลอง โครงสร้างและขั้นตอนการทำงานของระบบ และการออกแบบการวัดผลการทดลอง เพื่อประเมินประสิทธิภาพด้านการใช้งาน ด้านความปลอดภัย และความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อระบบพิสูจน์ตัวตนที่ได้ออกแบบ

## 3.1 ระเบียบวิธีการทดลอง

ระเบียบวิธีการทดลองของงานวิจัยนี้ ประกอบไปด้วย ตัวแปรและสมมติฐานที่ใช้ในการทดลอง รูปแบบการวิจัย กลุ่มตัวอย่างที่ใช้ในการวิจัย เครื่องมือที่ใช้ในการเก็บข้อมูล การเก็บรวบรวมข้อมูล โดยมีรายละเอียดดังนี้

### 3.1.1 ตัวแปรและสมมติฐาน

#### 3.1.1.1 ตัวแปรอิสระ (Independent Variable)

1. จำนวนรอบในการตั้งรหัสผ่าน คือ จำนวนรอบที่ใช้ในการตั้งรหัสผ่านรูปภาพในขั้นตอนการลงทะเบียน และรวมถึงจำนวนรอบที่ใช้ในการใส่รหัสผ่านรูปภาพในขั้นตอนการพิสูจน์ตัวตน โดยจำแนกตัวแปรได้ 2 ค่า ได้แก่ การใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ โดยตั้งรหัสผ่านทั้งหมด 8 รูปภาพ และการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ โดยตั้งรหัสผ่านรอบละ 4 รูปภาพ รวมทั้งหมด 8 รูปภาพ

2. การมีกฎในการเลือกรหัสผ่าน คือ กฎในการเลือกรูปภาพเป็นรหัสผ่าน โดยจะมีรูปภาพทั้งหมด 4 ประเภท ได้แก่ รูปภาพใบหน้าผู้ชาย รูปภาพใบหน้าผู้หญิง รูปภาพใบหน้าเด็ก และรูปภาพใบหน้าการ์ตูน โดยจำแนกตัวแปรได้ 2 ค่า ได้แก่ การมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ และการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

**3.1.1.2 ตัวแปรตาม (Dependent Variable)**

1. ประสิทธิภาพด้านการใช้งานของการพิสูจน์ตัวตนที่ได้ออกแบบในงานวิจัย ประกอบไปด้วย จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน

2. ประสิทธิภาพด้านความปลอดภัยของการพิสูจน์ตัวตนที่ได้ออกแบบในงานวิจัย ประกอบไปด้วย จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน

3. ความพึงพอใจของผู้ใช้ที่มีต่อระบบการพิสูจน์ตัวตนที่ได้ออกแบบในงานวิจัย วัดผลจากคะแนนแบบสอบถามความพึงพอใจที่ให้ผู้เข้าร่วมการทดลองตอบแบบสอบถามหลังทำการทดลองเสร็จสิ้น

**3.1.1.3 สมมติฐานในการทดลอง**

จำนวนรอบในการตั้งรหัสผ่าน และการมีกฎในการเลือกรหัสผ่าน มีผลต่อด้านการใช้งาน (Usability) และด้านความปลอดภัย (Security) ของรหัสผ่านรูปภาพ โดยมีสมมติฐานทั้งหมด 3 สมมติฐาน และมูลเหตุที่นำไปสู่สมมติฐานในงานวิจัยนี้ ดังต่อไปนี้

1. การเปรียบเทียบด้านการใช้งาน และด้านความปลอดภัย ระหว่างจำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และจำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ โดยในด้านการใช้งาน ผู้วิจัยมีแนวคิดว่าจากเดิมที่การพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่มีลักษณะแบบ S-Passface ต้องใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพถึง 2 รอบ อาจก่อให้เกิดความยุ่งยากซับซ้อน และมีการใช้เวลามาก และถ้ากำหนดให้ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพเพียง 1 รอบ จะสามารถเพิ่มการใช้งานให้ง่ายขึ้นได้ และในด้านความปลอดภัย ก็จะมีความปลอดภัยสูงขึ้น เนื่องจากเป็นการเพิ่มความเป็นไปได้ของรหัสผ่านอีกด้วย

$H_0$ : จำนวนรอบในการตั้งรหัสผ่าน ไม่มีอิทธิพลต่อการใช้งานรหัสผ่านรูปภาพ

$H_1$ : จำนวนรอบในการตั้งรหัสผ่าน มีอิทธิพลต่อการใช้งานรหัสผ่านรูปภาพ

$H_0$ : จำนวนรอบในการตั้งรหัสผ่าน ไม่มีอิทธิพลต่อความปลอดภัยของรหัสผ่านรูปภาพ

$H_1$ : จำนวนรอบในการตั้งรหัสผ่าน มีอิทธิพลต่อความปลอดภัยของรหัสผ่านรูปภาพ

2. การเปรียบเทียบด้านการใช้งาน และด้านความปลอดภัย ระหว่างการมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ และการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท โดยในด้านการใช้งาน ผู้วิจัยมีแนวคิดว่าจากเดิมที่การพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่มีลักษณะแบบ S-Passface จะมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ และถ้ากำหนดให้ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ก็จะไม่เกิดการบังคับผู้ใช้ที่ต้องเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ และไม่ต้องจดจำรูปภาพในทุกประเภท หรือผู้ใช้อาจไม่มีความสนใจต่อรูปภาพบางประเภทแต่ต้องเลือกก็จะส่งผลให้จดจำรหัสผ่านรูปภาพไม่ได้ และในด้านความปลอดภัย ก็จะมีความปลอดภัยสูงขึ้น เนื่องจากเป็นการเพิ่มความเป็นไปได้ของรหัสผ่านอีกด้วย

$H_0$ : การมีกฎในการเลือกรหัสผ่าน ไม่มีอิทธิพลต่อการใช้งานรหัสผ่านรูปภาพ

$H_1$ : การมีกฎในการเลือกรหัสผ่าน มีอิทธิพลต่อการใช้งานรหัสผ่านรูปภาพ

$H_0$ : การมีกฎในการเลือกรหัสผ่าน ไม่มีอิทธิพลต่อความปลอดภัยของรหัสผ่านรูปภาพ

$H_1$ : การมีกฎในการเลือกรหัสผ่าน มีอิทธิพลต่อความปลอดภัยของรหัสผ่านรูปภาพ

3. การเปรียบเทียบการมีอิทธิพลร่วมกัน ระหว่างจำนวนรอบในการตั้งรหัสผ่าน กับการมีกฎในการเลือกรหัสผ่าน ที่มีผลต่อด้านการใช้งาน และด้านความปลอดภัย

$H_0$ : จำนวนรอบในการตั้งรหัสผ่านร่วมกับการมีกฎในการเลือกรหัสผ่าน ไม่มีอิทธิพลต่อการใช้งานรหัสผ่านรูปภาพ

$H_1$ : จำนวนรอบในการตั้งรหัสผ่านร่วมกับการมีกฎในการเลือกรหัสผ่าน มีอิทธิพลต่อการใช้งานรหัสผ่านรูปภาพ

$H_0$ : จำนวนรอบในการใส่รหัสผ่านร่วมกับการมีกฎในการเลือกรหัสผ่าน ไม่มีอิทธิพลต่อความปลอดภัยของรหัสผ่านรูปภาพ

$H_1$ : จำนวนรอบในการใส่รหัสผ่านร่วมกับการมีกฎในการเลือกรหัสผ่านมีอิทธิพลต่อความปลอดภัยของรหัสผ่านรูปภาพ

### 3.1.2 รูปแบบการวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงทดลอง (Experimental Research) ใช้รูปแบบการทดลองแบบ 2x2 Between Subjects Design การทดลองจะแบ่งกลุ่มทดลองตามปัจจัยที่ศึกษา

ซึ่งแบ่งเป็น 4 กลุ่มทดลอง โดยให้แต่ละกลุ่มทดลองทำการทดลองกลุ่มละ 1 รูปแบบ โดยมีรูปแบบการทดลอง ดังตารางที่ 3.1

ตารางที่ 3.1

*รูปแบบการทดลองแบบ 2x2 Between Subjects Design*

| ปัจจัยที่ศึกษา | | จำนวนรอบในการตั้งรหัสผ่านรูปภาพ | |
|---|---|---|---|
| | | 1 รอบ | 2 รอบ |
| การมีกฎในการเลือกรหัสผ่านรูปภาพ | เลือกรหัสผ่านประเภทละ 2 รูปภาพ | กลุ่มทดลองที่ 1 | กลุ่มทดลองที่ 3 (มีลักษณะแบบเดียวกับ S-Passface) |
| | ไม่มีกฎในการเลือกรหัสผ่าน | กลุ่มทดลองที่ 2 | กลุ่มทดลองที่ 4 |

จากตารางที่ 3.1 เป็นการแสดงรูปแบบการทดลอง ประกอบไปด้วยกลุ่มทดลองทั้งหมด 4 กลุ่ม ได้แก่ กลุ่มทดลองที่ 1 ทำการทดลองการพิสูจน์ตัวตนโดยการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับการมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กลุ่มทดลองที่ 2 ทำการทดลองการพิสูจน์ตัวตนโดยการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท กลุ่มทดลองที่ 3 ทำการทดลองการพิสูจน์ตัวตนโดยการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับการมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ซึ่งเป็นรูปแบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่มีลักษณะแบบเดียวกับ S-Passface และกลุ่มทดลองที่ 4 ทำการทดลองการพิสูจน์ตัวตนโดยการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

### 3.1.3 กลุ่มตัวอย่างที่ใช้ในการวิจัย

การทดลองนี้ได้เลือกกลุ่มตัวอย่างแบบเจาะจง (Purposive sampling) เนื่องจากต้องมีการเก็บข้อมูลการทดลองซ้ำถึง 3 ครั้ง ได้แก่ ครั้งที่ 1 ทดลองการพิสูจน์ตัวตนหลังจากการลงทะเบียนทันที ครั้งที่ 2 ทดลองการพิสูจน์ตัวตนหลังจากการทะเบียนไปแล้ว 3 วัน และครั้งที่ 3 ทดลองการพิสูจน์ตัวตนหลังจากการลงทะเบียนไปแล้ว 15 วัน ดังนั้นผู้วิจัยจึงได้เลือกกลุ่มตัวอย่างเป็นเจ้าหน้าที่ในศาลอุทธรณ์ภาค 7 เพื่อให้สามารถติดตามเพื่อทำการทดลองทั้ง 3 ครั้งได้ โดยผู้วิจัย

มุ่งเน้นศึกษาเฉพาะกลุ่มตัวอย่าง ที่เคยใช้งานระบบพิสูจน์ตัวตนและ ใช้งานคอมพิวเตอร์มาแล้วอย่างน้อย 1 ปี ทั้งเพศชาย และเพศหญิง จำนวนทั้งหมด 60 คน โดยได้ทำการสุ่มเพื่อแบ่งกลุ่มทดลองออกเป็น 4 กลุ่ม กลุ่มละ 15 คน โดยแต่ละกลุ่มทดลองจะเข้ารับการทดลองการพิสูจน์ตัวตนกลุ่มละ 1 รูปแบบ ซึ่งผู้เข้าร่วมการทดลองทุกคนจะได้รับหน้าที่เป็นทั้งผู้ใช้งานการพิสูจน์ตัวตนเพื่อทำการทดลองด้านการใช้งาน และเป็นผู้โจรกรรมเพื่อทำการทดลองด้านความปลอดภัย

### 3.1.4 เครื่องมือที่ใช้ในการเก็บข้อมูล

เครื่องมือที่ใช้ในการเก็บข้อมูลการทดลอง ได้แก่ เครื่องคอมพิวเตอร์ชนิดพกพา หน่วยประมวลผลกลาง Intel® Core™ i5 2.30 GHz หน่วยความจำหลัก 6 GB หน่วยจัดเก็บข้อมูล 500 GB จอภาพแบบ WLED ขนาด 15.6 นิ้ว ความละเอียดของจอภาพ 1366x768 พิกเซล ระบบปฏิบัติการ Windows 7 64-bit โปรแกรมที่ใช้ในการทดลองพัฒนาด้วยภาษา ASP.NET (C#.NET) โดยโปรแกรม Microsoft Visual Studio 2010 ใช้ระบบจัดการฐานข้อมูล Microsoft SQL Server 2008 ในการจัดเก็บข้อมูล ประมวลผลด้วยโปรแกรม Internet Explorer 11 ในส่วนของการเก็บข้อมูลทั่วไปและข้อมูลความพึงพอใจของผู้เข้าร่วมการทดลองจะใช้แบบสอบถามข้อมูลทั่วไปและแบบสอบถามความพึงพอใจผ่านโปรแกรม Internet Explorer 11 เพื่อบันทึกลงฐานข้อมูล

### 3.1.5 การเก็บรวบรวมข้อมูล

งานวิจัยนี้ ทำการเก็บข้อมูลโดยเริ่มจากข้อมูลทั่วไปของผู้เข้าร่วมการทดลองจากการตอบแบบสอบถามข้อมูลทั่วไปก่อนการทดลอง ข้อมูลด้านการใช้งานโดยการเก็บข้อมูลจากการทดลองการพิสูจน์ตัวตน ข้อมูลด้านความปลอดภัยโดยการเก็บข้อมูลจากการทดลองการโจรกรรมการพิสูจน์ตัวตน และข้อมูลด้านความพึงพอใจจากการตอบแบบสอบถามความพึงพอใจหลังการทดลองในครั้งสุดท้าย ซึ่งการทดลองด้านการใช้งานและด้านความปลอดภัยจะทำการทดลองทั้งหมด 3 ครั้ง ได้แก่ ครั้งที่ 1 ทดลองหลังจากการลงทะเบียนทันที ครั้งที่ 2 ทดลองหลังจากการทะเบียนไปแล้ว 3 วัน และครั้งที่ 3 ทดลองหลังจากการลงทะเบียนไปแล้ว 15 เพื่อวัดความสามารถในการจำได้ (Retention over time) โดยการทดลองนี้ใช้เวลาในการเก็บข้อมูลทั้งหมด 3 สัปดาห์ และงานวิจัยใช้ห้องประชุมศาลอุทธรณ์ภาค 7 ชั้น 5 ในการเก็บรวบรวมข้อมูล

เพื่อให้การทดลองการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพของงานวิจัยนี้ ได้ข้อมูลการใช้งานระบบพิสูจน์ตัวตนที่เสมือนการใช้งานจริง ผู้วิจัยจึงได้นำโปรแกรมการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่ได้ออกแบบมาใช้ร่วมกับการตอบแบบสอบถามการใช้งานระบบอินทราเน็ต (Intranet) ของศาลอุทธรณ์ภาค 7 ในการทดลองครั้งที่ 1 แบบสอบถามความพึงพอใจต่อระบบคอมพิวเตอร์และระบบเครือข่ายในศาลอุทธรณ์ภาค 7 ในการทดลองครั้งที่ 2 และแบบสำรวจความ

ต้องการในการอบรมด้านเทคโนโลยีสารสนเทศในศาลอุทธรณ์ภาค 7 ในการทดลองครั้งที่ 3 เพื่อให้ผู้เข้าร่วมการทดลองให้ความสำคัญในการพิสูจน์ตัวตน และเกิดความพยายามในการจดจำรหัสผ่านเพื่อจะได้ผ่านเข้าไปทำแบบสอบถามดังกล่าวได้ เพราะแบบสอบถามดังกล่าวจะส่งผลต่อการพัฒนาระบบเทคโนโลยีสารสนเทศของศาลอุทธรณ์ภาค 7 และการจัดสรรครุภัณฑ์คอมพิวเตอร์ให้กับบุคลากรในศาลอุทธรณ์ภาค 7 ร่วมถึงการจัดอบรมด้านเทคโนโลยีสารสนเทศเพื่อนำไปจัดทำแผนพัฒนารายบุคคล (IDP : Individual Development Planning) ของสำนักงานศาลยุติธรรม

## 3.2 โครงสร้างและขั้นตอนการทำงานของระบบ

โครงสร้างและขั้นตอนการทำงานของระบบ ในหัวข้อนี้จะอธิบายถึง การออกแบบโปรแกรมสำหรับการทดลอง และขั้นตอนการทำงานของระบบโดยแบ่งออกเป็น 2 ขั้นตอน ได้แก่ ขั้นตอนการลงทะเบียน (Register) และขั้นตอนการเข้าสู่ระบบ (Login) โดยมีรายละเอียดดังนี้

### 3.2.1 การออกแบบโปรแกรมสำหรับการทดลอง

การออกแบบโปรแกรมการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่ใช้ในการทดลองของงานวิจัยนี้ ได้นำเอารูปแบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพของ S-Passface มาประยุกต์ใช้ในการออกแบบตามปัจจัยที่ศึกษา ได้แก่ ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน ระหว่าง การใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ โดยตั้งรหัสผ่านทั้งหมด 8 รูปภาพ กับการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ โดยตั้งรหัสผ่านรอบละ 4 รูปภาพ รวมทั้งหมด 8 รูปภาพ และการมีกฎในการเลือกรหัสผ่านรูปภาพ ระหว่าง การมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ผู้วิจัยจึงได้ออกแบบโปรแกรม ซึ่งแบ่งได้เป็น 2 โปรแกรม ได้แก่ โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ดังภาพที่ 3.1 และโปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ดังภาพที่ 3.2-3.3 โดยในกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ โปรแกรมจะทำการตรวจสอบว่าผู้เข้าร่วมการทดลองเลือกรูปภาพตามกฎที่ได้กำหนดหรือไม่ การตั้งรหัสผ่านจะใช้รูปภาพทั้งหมด 8 รูปภาพ จากรูปภาพตัวเลือกสำหรับใช้สร้างเป็นรหัสผ่านทั้งหมด 36 รูปภาพ แบ่งประเภทของรูปภาพออกเป็น 4 ประเภท ประเภทละ 9 รูปภาพ ได้แก่ รูปภาพใบหน้าผู้ชาย รูปภาพใบหน้าผู้หญิง รูปภาพใบหน้าเด็ก และรูปภาพใบหน้าตัวการ์ตูน โดยรูปภาพแต่ละประเภทจะจัดเรียงเป็น 3 แถว แถวละ 3 รูปภาพ ในการเลือกรหัสผ่านรูปภาพจะใช้คีย์บอร์ดพิมพ์ตัวอักษรที่โปรแกรมทำการสุ่มจำนวน 2 ตัวอักษร ที่แสดงอยู่ใต้รูปภาพ ซึ่งการพิมพ์ตัวอักษรเพื่อเลือกรูปภาพแต่ละรูปภาพโปรแกรมจะทำการตรวจสอบว่า มีการพิมพ์ตัวอักษรเพื่อเลือกรูปภาพซ้ำหรือไม่ เนื่องจากไม่สามารถเลือกรูปภาพซ้ำได้ และมีการ

พิมพ์ตัวอักษรถูกต้องตามที่ได้สุ่มมาแสดงหรือไม่ ถ้าไม่ถูกต้องระบบจะทำการลบตัวอักษรที่พิมพ์ซ้ำหรือพิมพ์ผิดทันที และจะมีการแจ้งเตือนให้พิมพ์ตัวอักษรใหม่ให้ถูกต้อง ส่วนการยกเลิกรูปภาพที่เลือกไปแล้วสามารถใช้ปุ่ม Backspace ที่คีย์บอร์ดลบตัวอักษรของรูปภาพที่ต้องการยกเลิกได้ หรือถ้าต้องการยกเลิกการเลือกรูปภาพทั้งหมดสามารถกดปุ่มยกเลิกในหน้าจอโปรแกรมได้เลย ในการออกแบบโปรแกรมตามปัจจัยที่ศึกษาก็เพื่อหารูปแบบในการออกแบบวิธีการพิสูจน์ตัวตนที่เหมาะสมให้มีการใช้งานที่ง่าย (Usability) มีความปลอดภัย (Security) และผู้ใช้มีความพึงพอใจ


*ภาพที่ 3.1* หน้าจอโปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ


*ภาพที่ 3.2* หน้าจอโปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ (รอบที่ 1)


*ภาพที่ 3.3* หน้าจอโปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ (รอบที่ 2)

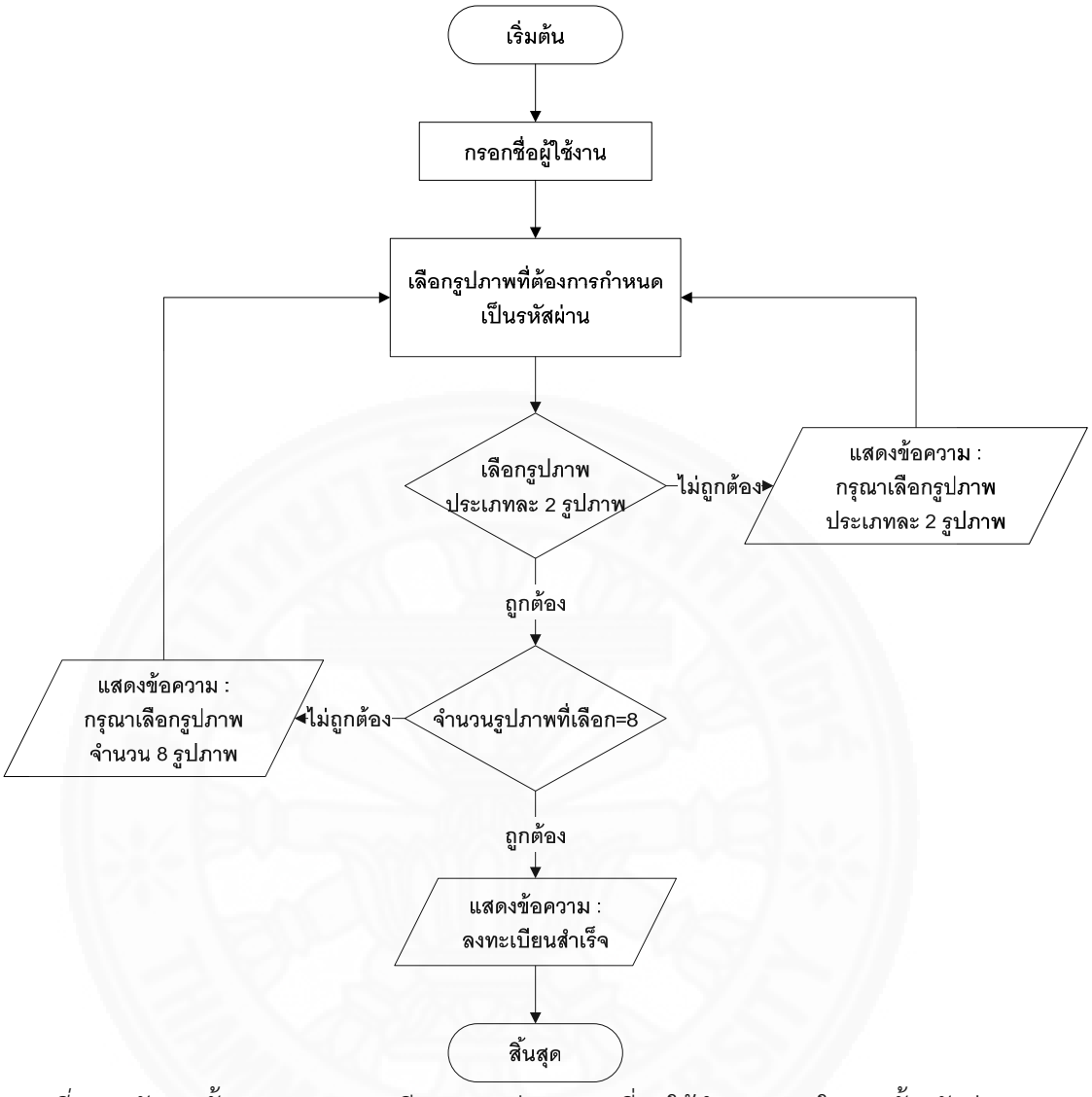
### 3.2.2 ขั้นตอนการทำงานของระบบ

ขั้นตอนการทำงานของระบบสามารถอธิบายโดยแบ่งออกเป็น 2 ขั้นตอน ได้แก่ ขั้นตอนการลงทะเบียน (Register) และขั้นตอนการเข้าสู่ระบบ (Login) ดังนี้

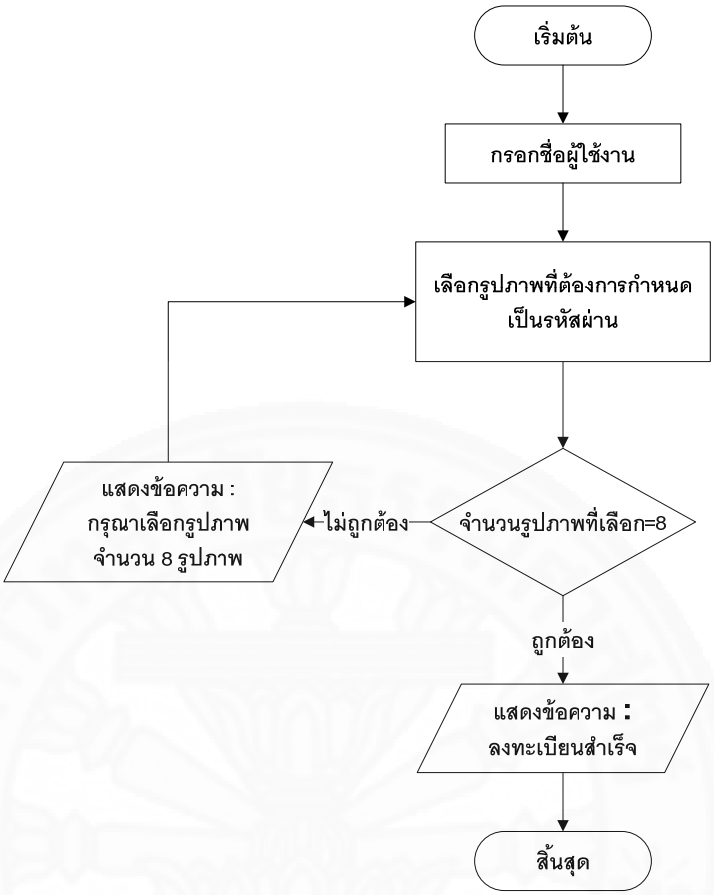
**3.2.2.1 ขั้นตอนการลงทะเบียน (Register)**

ขั้นตอนการลงทะเบียนจะมีวิธีการแตกต่างกันตามโปรแกรมที่ได้ออกแบบตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยแบ่งออกเป็น 2 โปรแกรม ได้แก่ โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และโปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ โดยมีขั้นตอนการทำงาน ดังนี้

1. โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ เริ่มจากให้ผู้เข้าร่วมการทดลองกรอกชื่อผู้ใช้งาน ซึ่งผู้วิจัยได้กำหนดไว้ให้ หลังจากนั้นให้ผู้เข้าร่วมการทดลองพิมพ์ตัวอักษรที่อยู่ใต้รูปภาพที่ต้องการเลือกเป็นรหัสผ่าน ทั้งหมด 8 รูปภาพ ในกรณีกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ให้ผู้เข้าร่วมการทดลองเลือกรูปภาพจากประเภทของรูปภาพทั้ง 4 ประเภท ๆ ละ 2 รูปภาพ จนครบ 8 รูปภาพ และในกรณีกลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท ให้ผู้เข้าร่วมการทดลองเลือกรูปภาพจากประเภทของรูปภาพใดก็ได้จนครบ 8 รูปภาพ เมื่อเลือกรูปภาพเสร็จเรียบร้อยแล้วให้คลิกปุ่มยืนยันการลงทะเบียนเป็นอันเสร็จสิ้นขั้นตอนการลงทะเบียน

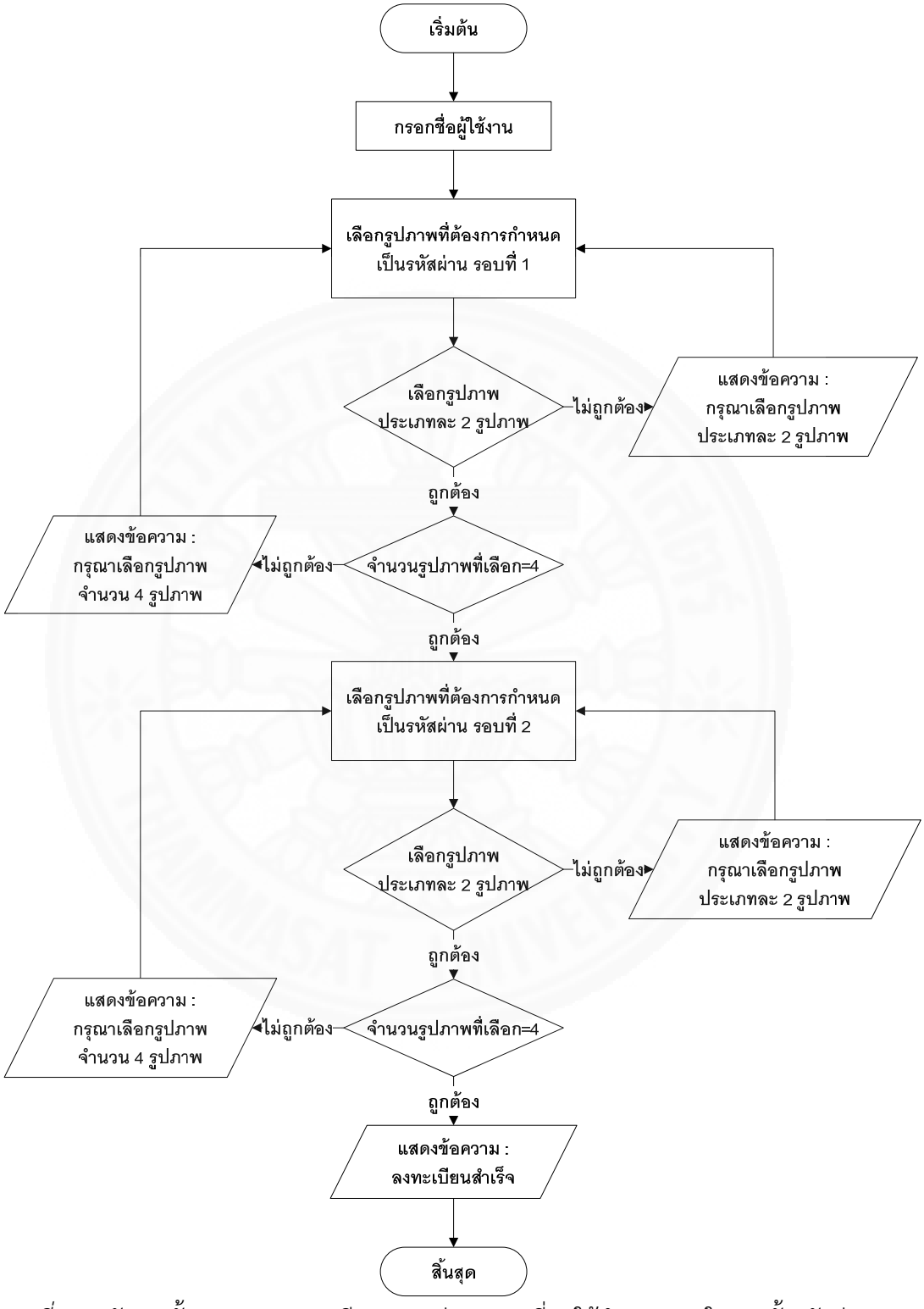



*ภาพที่ 3.4* ผังงานขั้นตอนการลงทะเบียนของกลุ่มทดลองที่ 1 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับการมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ

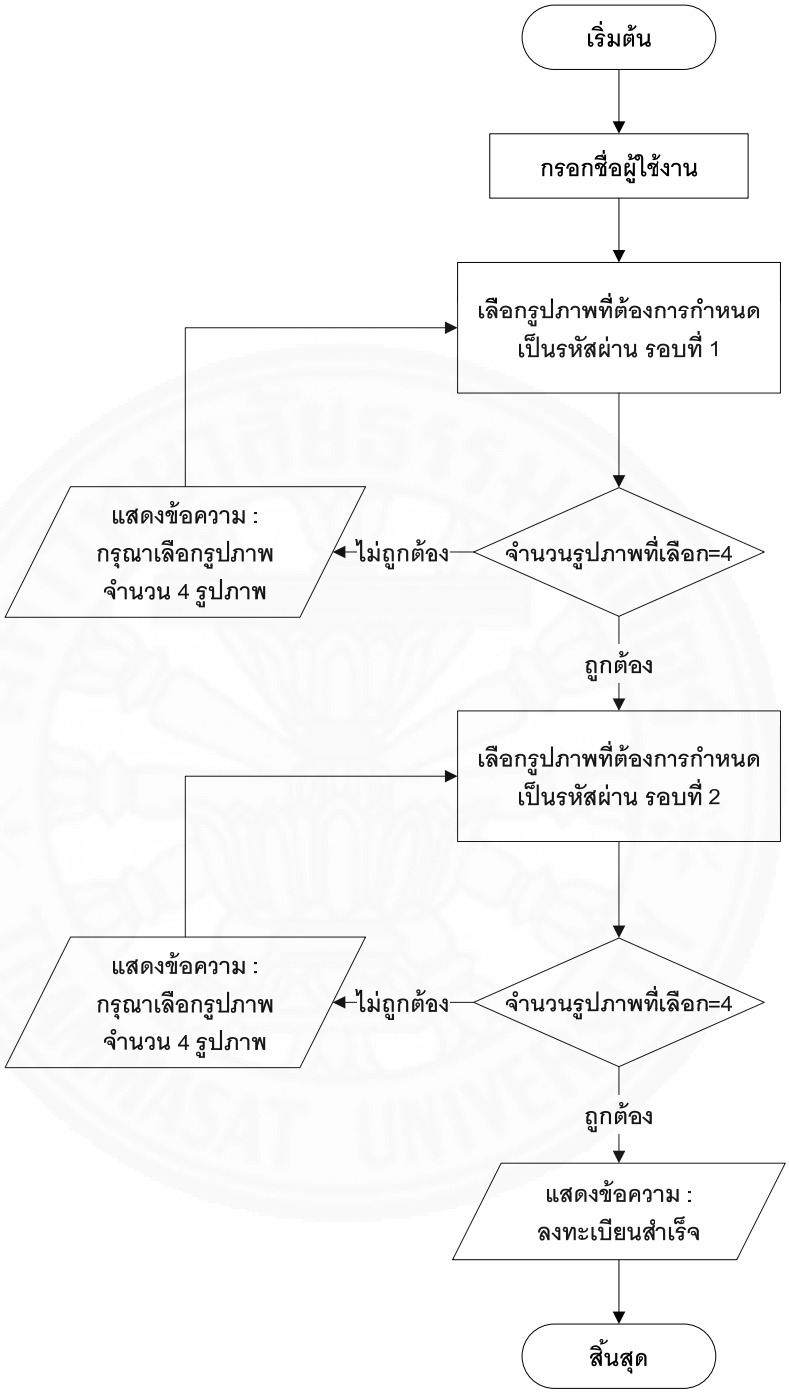



*ภาพที่ 3.5* ผังงานขั้นตอนการลงทะเบียนของกลุ่มทดลองที่ 2 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

2. โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ เริ่มจากให้ผู้เข้าร่วมการทดลองกรอกชื่อผู้ใช้งาน ซึ่งผู้วิจัยกำหนดไว้ให้ หลังจากนั้นให้ผู้เข้าร่วมการทดลองพิมพ์ตัวอักษรที่อยู่ใต้รูปภาพที่ต้องการเลือกเป็นรหัสผ่าน ซึ่งได้แบ่งการตั้งรหัสผ่านออกเป็น 2 รอบ ๆ ละ 4 รูปภาพ โดยในแต่ละรอบจะมีประเภทของรูปภาพให้เลือกรอบละ 2 ประเภท ในกรณีกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านประเภทละ 2 รูปภาพนั้น ให้ผู้เข้าร่วมการทดลองเลือกรูปภาพประเภทละ 2 รูปภาพ ทั้ง 2 รอบ จนครบ 8 รูปภาพ และในกรณีกลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท ให้ผู้เข้าร่วมการทดลองเลือกรูปภาพจากประเภทของรูปภาพใดก็ได้ทั้ง 2 รอบ จนครบ 8 รูปภาพ โดยเมื่อสร้างรหัสผ่านรอบที่ 1 เสร็จเรียบร้อยแล้วให้คลิกปุ่มคลิกเพื่อสร้างรหัสผ่านส่วนถัดไป เพื่อสร้างรหัสผ่านในรอบที่ 2 และเมื่อสร้างรหัสผ่านในรอบที่ 2 เสร็จเรียบร้อยแล้วให้คลิกปุ่มยืนยันการลงทะเบียน เป็นอันเสร็จสิ้นขั้นตอนการลงทะเบียน




*ภาพที่ 3.6* ผังงานขั้นตอนการลงทะเบียนของกลุ่มทดลองที่ 3 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับการมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ




*ภาพที่ 3.7* ผังงานขั้นตอนการลงทะเบียนของกลุ่มทดลองที่ 4 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับการไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

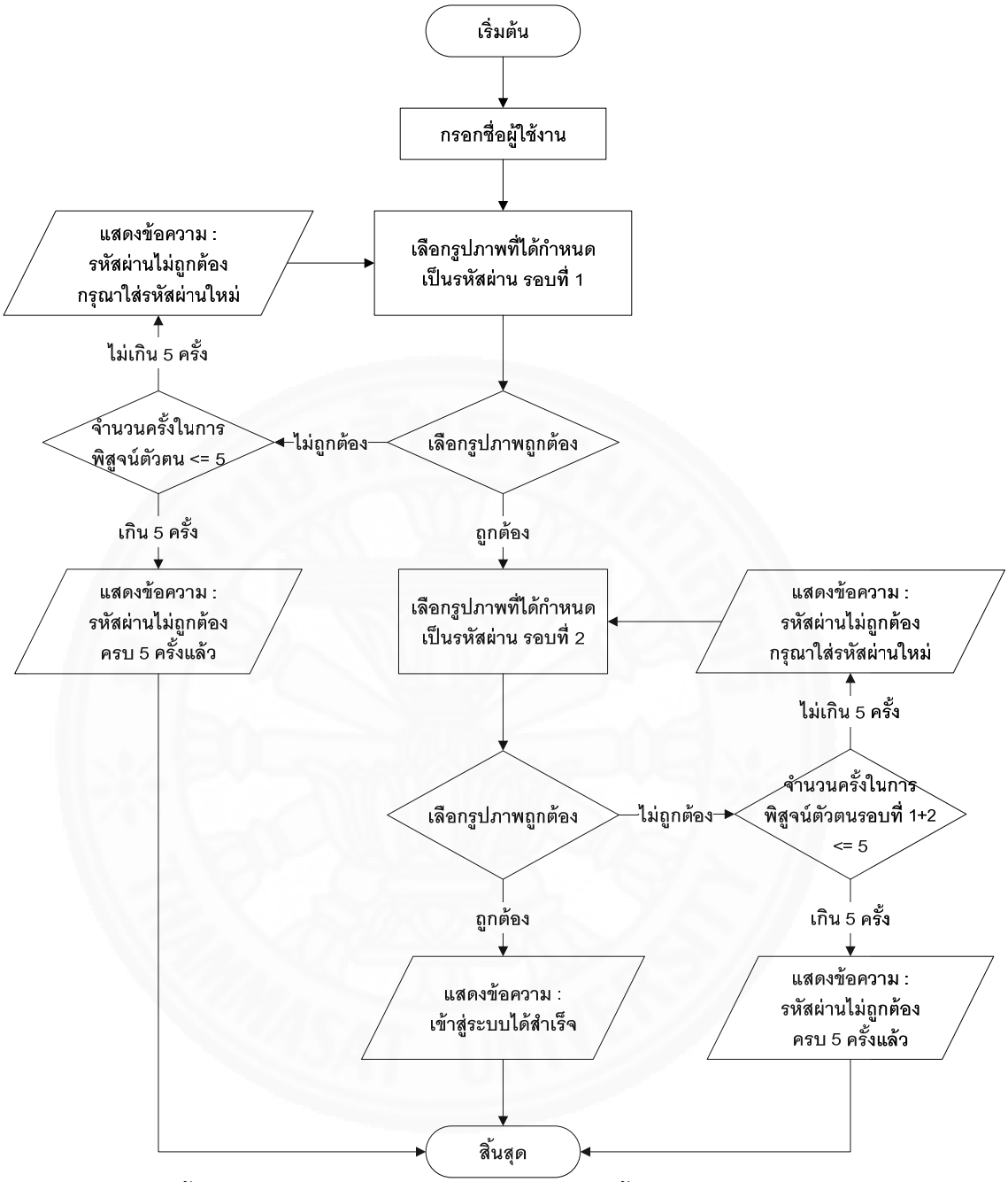
**3.2.2.2 ขั้นตอนการเข้าสู่ระบบ (Login)**

ขั้นตอนการเข้าสู่ระบบ ก็จะแตกต่างกันไปตามโปรแกรมที่ได้ออกแบบตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านรูปภาพ โดยแบ่งออกเป็น 2 โปรแกรม ได้แก่ โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และโปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ โดยมีขั้นตอนการทำงาน ดังนี้

1. โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ เริ่มจากให้ผู้เข้าร่วมการทดลองกรอกชื่อผู้ใช้งาน แล้วให้ทำการพิสูจน์ตัวตนโดยการพิมพ์ตัวอักษรที่อยู่ใต้รูปภาพที่ได้เลือกเป็นรหัสผ่านไว้ในขั้นตอนการลงทะเบียน ทั้งหมด 8 รูปภาพ เมื่อใส่รหัสผ่านรูปภาพเสร็จเรียบร้อยแล้วให้คลิกปุ่มเข้าสู่ระบบ ถ้าผู้เข้าร่วมการทดลองใส่รหัสผ่านรูปภาพถูกต้องและลำดับในการเลือกรูปภาพถูกต้องตามที่ได้สร้างไว้ในขั้นตอนการลงทะเบียน ก็จะสามารถเข้าสู่ระบบได้สำเร็จ โดยผู้เข้าร่วมการทดลองจะมีโอกาสในการพิสูจน์ตัวตนทั้งหมด 5 ครั้ง หากทำการพิสูจน์ตัวตนสำเร็จก่อนครบ 5 ครั้ง จะผ่านขั้นตอนการพิสูจน์ตัวตนทันที หรือหากทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง

2. โปรแกรมที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ เริ่มจากให้ผู้เข้าร่วมการทดลองกรอกชื่อผู้ใช้งาน แล้วให้ทำการพิสูจน์ตัวตนโดยการพิมพ์ตัวอักษรที่อยู่ใต้รูปภาพที่ได้เลือกเป็นรหัสผ่านไว้ในขั้นตอนการลงทะเบียน โดยแบ่งเป็น 2 รอบ เมื่อใส่รหัสผ่านรูปภาพรอบที่ 1 เสร็จเรียบร้อยแล้วให้คลิกปุ่มคลิกเพื่อใส่รหัสผ่านส่วนถัดไป ถ้าผู้เข้าร่วมการทดลองใส่รหัสผ่านรูปภาพถูกต้องและลำดับในการเลือกรูปภาพถูกต้องตามที่ได้สร้างไว้ในขั้นตอนการลงทะเบียน ก็จะสามารถผ่านไปใส่รหัสผ่านรูปภาพในรอบที่ 2 ได้ และเมื่อใส่รหัสผ่านรูปภาพในรอบที่ 2 เสร็จเรียบร้อยแล้วให้คลิกปุ่มเข้าสู่ระบบ ถ้าผู้เข้าร่วมการทดลองใส่รหัสผ่านรูปภาพถูกต้องและลำดับในการเลือกรูปภาพถูกต้องตามที่ได้สร้างไว้ในขั้นตอนการลงทะเบียน ก็จะสามารถเข้าสู่ระบบได้สำเร็จ ผู้เข้าร่วมการทดลองจะมีโอกาสในการพิสูจน์ตัวตนรวมทั้ง 2 รอบ ทั้งหมด 5 ครั้ง หากทำการพิสูจน์ตัวตนสำเร็จก่อนครบ 5 ครั้ง จะผ่านขั้นตอนการพิสูจน์ตัวตนทันที หรือหากทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง


*ภาพที่ 3.8* ผังงานขั้นตอนการเข้าสู่ระบบที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ




*ภาพที่ 3.9* ผังงานขั้นตอนการเข้าสู่ระบบที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ

### 3.3 การออกแบบการทดลองและการวัดผล

การออกแบบการทดลองและการวัดผล จะอธิบายถึง รายละเอียดของการออกแบบการทดลองด้านการใช้งาน (Usability) ด้านความปลอดภัย (Security) การออกแบบแบบสอบถาม และการนำผลการทดลองที่ได้มาวัดผล โดยมีรายละเอียดดังนี้

### 3.3.1 การออกแบบการทดลอง

งานวิจัยนี้ได้กำหนดรูปแบบการทดลองออกเป็น 4 กลุ่ม ตามปัจจัยที่ศึกษา โดยการทดลองจะทำการทดลองทีละ 1 คู่ ประกอบด้วย ผู้ที่รับหน้าที่ทำการทดลองการพิสูจน์ตัวตนเพื่อเก็บข้อมูลด้านการใช้งาน และผู้ที่รับหน้าที่ทำการทดลองการโจรกรรมการพิสูจน์ตันตนเพื่อเก็บข้อมูลด้านความปลอดภัย โดยมีรายละเอียดดังนี้

#### 3.3.1.1 การทดลองด้านการใช้งาน (Usability)

การทดลองด้านการใช้งานเริ่มจากผู้วิจัยอธิบายวัตถุประสงค์และรายละเอียดการทดลองให้ผู้เข้าร่วมการทดลองทราบ แล้วจึงเริ่มทำการทดลอง โดยจะทำการทดลองทั้งหมด 3 ครั้ง ได้แก่ ครั้งที่ 1 ทำการทดลองการพิสูจน์ตัวตนหลังจากการลงทะเบียนทันที ครั้งที่ 2 ทำการทดลองการพิสูจน์ตัวตนหลังจากการทะเบียนไปแล้ว 3 วัน และครั้งที่ 3 ทำการทดลองการพิสูจน์ตัวตนหลังจากการลงทะเบียนไปแล้ว 15 วัน รายละเอียดดังนี้

การทดลองครั้งที่ 1 ทดลองการพิสูจน์ตัวตนหลังจากการลงทะเบียนทันที โดยเริ่มจากให้ผู้เข้าร่วมการทดลองตอบแบบสอบถามข้อมูลทั่วไป ตามด้วยผู้วิจัยจะสาธิตการใช้งานโปรแกรมที่ได้ออกแบบและให้ผู้เข้าร่วมการทดลองได้ทดลองใช้งาน เมื่อผู้เข้าร่วมการทดลองเข้าใจวิธีการใช้งานโปรแกรมและเกิดความคุ้นเคยแล้ว ก็จะให้ทำการทดลองโดยเริ่มจากการลงทะเบียนเพื่อตั้งรหัสผ่านรูปภาพ โดยผู้วิจัยขอความร่วมมือไม่ให้ทำการจดรหัสผ่าน และเมื่อลงทะเบียนเสร็จเรียบร้อยแล้ว ให้ทำการพิสูจน์ตัวตนทันที เพื่อเข้าไปทำแบบสอบถามการใช้งานระบบอินทราเน็ต (Intranet) ของศาลอุทธรณ์ภาค 7

การทดลองครั้งที่ 2 ทดลองการพิสูจน์ตัวตนหลังจากการทะเบียนไปแล้ว 3 วัน โดยให้ผู้เข้าร่วมการทดลองด้านการใช้งานทำการพิสูจน์ตัวตนเพื่อเข้าไปทำแบบสอบถามความพึงพอใจต่อระบบคอมพิวเตอร์และระบบเครือข่ายของศาลอุทธรณ์ภาค 7

การทดลองครั้งที่ 3 ทดลองการพิสูจน์ตัวตนหลังจากการลงทะเบียนไปแล้ว 15 วัน โดยให้ผู้เข้าร่วมการทดลองด้านการใช้งานทำการพิสูจน์ตัวตนเพื่อเข้าไปทำแบบสำรวจความต้องการในการอบรมด้านเทคโนโลยีสารสนเทศในศาลอุทธรณ์ภาค 7 และแบบสอบถามความพึงพอใจต่อโปรแกรมการพิสูจน์ตัวตนจากการทดลองนี้ตามที่ได้ผู้วิจัยได้จัดทำขึ้น

โดยการทดลองด้านการใช้งานจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง

**3.3.1.2 การทดลองด้านความปลอดภัย (Security)**

ในการทดลองด้านความปลอดภัย ให้ผู้เข้าร่วมการทดลองที่รับหน้าที่ทำการโจรกรรมการพิสูจน์ตัวตน โดยใช้วิธีการแอบมอง (Shoulder surfing) พยายามแอบมองรหัสผ่านในขณะที่ผู้เข้าร่วมการทดลองด้านการใช้งานกำลังทำการพิสูจน์ตัวตน โดยสามารถใช้วิธีการจดรหัสผ่าน หรือการถ่ายรูปภาพก็ได้ แต่ผู้โจรกรรมต้องอยู่ห่างจากหน้าจอคอมพิวเตอร์โดยมีระยะห่างไม่ต่ำกว่า 1 เมตร เมื่อผู้เข้าร่วมการทดลองด้านการใช้งานพิสูจน์ตัวตนเสร็จสิ้น จะให้ผู้ที่รับหน้าที่โจรกรรมการพิสูจน์ตัวตน นำรหัสผ่านที่โจรกรรมได้มาทำการพิสูจน์ตัวตน โดยให้โอกาสทำการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากทำการโจรกรรมการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง การทดลองด้านความปลอดภัยจะทำการทดลองทั้งหมด 3 ครั้ง เช่นเดียวกับผู้เข้าร่วมการทดลองด้านการใช้งาน

**3.3.2 การออกแบบแบบสอบถาม**

แบบสอบถามที่ได้ออกแบบเพื่อใช้ในการเก็บข้อมูลของผู้เข้าร่วมการทดลองในการทดลองนั้น ผู้วิจัยได้แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 แบบสอบถามข้อมูลทั่วไป ได้แก่ คำถามเกี่ยวกับลักษณะทางประชากรศาสตร์ เช่น เพศ อายุ และระดับการศึกษา เป็นต้น และคำถามเกี่ยวกับพฤติกรรมการใช้ระบบพิสูจน์ตัวตน เช่น ความถี่ในการใช้คอมพิวเตอร์ วิธีการพิสูจน์ตัวตนที่เคยใช้ วิธีการตั้งรหัสผ่าน วิธีเก็บรักษารหัสผ่าน และความถี่ในการลืมรหัสผ่าน เป็นต้น

ส่วนที่ 2 แบบสอบถามความพึงพอใจที่มีต่อโปรแกรมการพิสูจน์ตัวตนได้ออกแบบตามมาตรฐาน ISO (Lashkari, 2010) โดยใช้แบบสอบถามแบบมาตราส่วนประมาณค่า (Rating scale) โดยแบ่งระดับคะแนนความพึงพอใจ เป็น 5 ระดับ ดังนี้

| | | |
|---|---|---|
| 5 | หมายถึง | ระดับความพึงพอใจมากที่สุด |
| 4 | หมายถึง | ระดับความพึงพอใจมาก |
| 3 | หมายถึง | ระดับความพึงพอใจปานกลาง |
| 2 | หมายถึง | ระดับความพึงพอใจน้อย |
| 1 | หมายถึง | ระดับความพึงพอใจน้อยที่สุด |

ส่วนที่ 3 ข้อคิดเห็นและข้อเสนอแนะเพิ่มเติมเกี่ยวกับโปรแกรมการพิสูจน์ตัวตนที่ออกแบบ

**3.3.3 การนำผลการทดลองที่ได้มาวัดผล**

งานวิจัยนี้จะนำผลการทดลองที่ได้จากการทดลองและการตอบแบบสอบถามมาประมวลผลด้วยโปรแกรมสำเร็จรูปสำหรับวิเคราะห์ข้อมูลทางสถิติ SPSS/PC โดยจะวิเคราะห์ผลการทดลองด้วยวิธีการ Two-way ANOVA โดยผลการทดลองที่ได้ วัดจากข้อมูลในการทดลอง ดังนี้

### 3.3.3.1 การวัดผลการทดลองด้านการใช้งาน (Usability)

#### (1) ความสำเร็จในการพิสูจน์ตัวตน

โดยกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง หากทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง ซึ่งระบบจะเก็บจำนวนครั้งที่ผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนสำเร็จ โดยข้อมูลร้อยละของความสำเร็จในการพิสูจน์ตัวตน วัดจากจำนวนครั้งที่ทำการพิสูจน์ตัวตนสำเร็จของผู้เข้าร่วมการทดลอง โดยใช้สูตรคำนวณ (ดนุพัฒน์ กชชาดาปภาดา, 2556) ดังนี้

$$ASR_{aut} = \frac{\sum_{i,j=1}^{i=5,j=15}(w_i \times n_j) \times \sum n_{ij}}{5}$$

เมื่อ $ASR_{aut}$ คือ อัตราความสำเร็จในการพิสูจน์ตัวตน (ร้อยละ)

w คือ ระดับคะแนนของการพิสูจน์ตัวตนสำเร็จ

n คือ จำนวนผู้เข้าร่วมการทดลองที่พิสูจน์ตัวตนสำเร็จ

i คือ จำนวนครั้งที่ในการพิสูจน์ตัวตน

j คือ จำนวนผู้เข้าร่วมการทดลอง

โดยระดับคะแนนของการพิสูจน์ตัวตนสำเร็จ จะแบ่งออกได้ ดังนี้

| | |
|---|---|
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 1 | ได้ 5 คะแนน |
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 2 | ได้ 4 คะแนน |
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 3 | ได้ 3 คะแนน |
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 4 | ได้ 2 คะแนน |
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 5 | ได้ 1 คะแนน |
| พิสูจน์ตัวตนไม่สำเร็จ | ได้ 0 คะแนน |

#### (2) เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน

โดยจะเก็บเวลาต่อเนื่องตั้งแต่ผู้เข้าร่วมการทดลองเริ่มทำการพิสูจน์ตัวตนจนสิ้นสุดการทดลอง โดยข้อมูลเวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน วัดจากค่าเฉลี่ยของเวลาที่ใช้ทั้งหมดของผู้เข้าร่วมการทดลอง โดยใช้สูตรคำนวณ (ดนุพัฒน์ กชชาดาปภาดา, 2556) ดังนี้

$$AVT_{aut} = \frac{\sum_{i=1}^{N} t}{\mathrm{N}}$$

เมื่อ $ASR_{aut}$ คือ ค่าเฉลี่ยของเวลาที่ใช้ในการพิสูจน์ตัวตน (วินาที)

t คือ ผลรวมของเวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตนสำเร็จ

N คือ จำนวนผู้เข้าร่วมการทดลองแต่ละกลุ่มการทดลอง

#### 3.3.3.2 การวัดผลการทดลองด้านความปลอดภัย (Security)

**(1) ความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน**

โดยกำหนดให้ผู้เข้าร่วมการทดลองนำรหัสผ่านที่โจรกรรมได้มาทำการพิสูจน์ตัวตน โดยให้โอกาสทำการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากทำการโจรกรรมการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง ซึ่งจะเก็บจำนวนครั้งที่ผู้เข้าร่วมการทดลองทำการโจรกรรมสำเร็จ โดยข้อมูลร้อยละของความสำเร็จในการโจรกรรมพิสูจน์ตัวตน วัดจากจำนวนครั้งที่ใช้ในการโจรกรรมสำเร็จ โดยใช้สูตรคำนวณ (ดนุพัฒน์ กชชาดาปภาดา, 2556) ดังนี้

$$ASR_{sfaut} = \frac{\sum_{i,j=1}^{i=5,j=15}(w_i \times n_j) \times \sum n_{ij}}{5}$$

เมื่อ $ASR_{sfaut}$ คือ อัตราความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน (ร้อยละ)

w คือ ระดับคะแนนของการโจรกรรมการพิสูจน์ตัวตนสำเร็จ

n คือ จำนวนผู้เข้าร่วมการทดลองที่โจรกรรมสำเร็จ

i คือ จำนวนครั้งที่ในการโจรกรรม

j คือ จำนวนผู้เข้าร่วมการทดลอง

โดยระดับคะแนนของการโจรกรรมการพิสูจน์ตัวตนสำเร็จ จะแบ่งออกได้ ดังนี้

| | |
|---|---|
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 1 | ได้ 5 คะแนน |
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 2 | ได้ 4 คะแนน |
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 3 | ได้ 3 คะแนน |
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 4 | ได้ 2 คะแนน |
| พิสูจน์ตัวตนสำเร็จในครั้งที่ 5 | ได้ 1 คะแนน |
| พิสูจน์ตัวตนไม่สำเร็จ | ได้ 0 คะแนน |

**(2) เวลาเฉลี่ยที่ใช้ในการโจรกรรมพิสูจน์ตัวตน**

โดยจะเก็บเวลาต่อเนื่องตั้งแต่ผู้เข้าร่วมการทดลองเริ่มทำการพิสูจน์ตัวตนจนสิ้นสุดการทดลอง โดยข้อมูลเวลาเฉลี่ยที่ใช้ในการโจรกรรมพิสูจน์ตัวตน วัดจากค่าเฉลี่ยของเวลาที่ใช้ทั้งหมด โดยใช้สูตรคำนวณ (ดนุพัฒน์ กชชาดาปภาดา, 2556) ดังนี้

$$AVT_{sfaut} = \frac{\sum_{i=1}^{N} t}{\mathrm{N}}$$

เมื่อ $ASR_{sfaut}$ คือ ค่าเฉลี่ยของเวลาที่ใช้ในการโจรกรรมพิสูจน์ตัวตน (วินาที)

t คือ ผลรวมของเวลาเฉลี่ยที่ใช้ในการโจรกรรมพิสูจน์ตัวตน

N คือ จำนวนผู้เข้าร่วมการทดลองแต่ละกลุ่มการทดลอง

### 3.3.3.3 การวัดผลความพึงพอใจ

โดยการวัดผลความพึงพอใจของผู้ใช้ที่มีต่อระบบการพิสูจน์ตัวตนที่ได้ออกแบบในงานวิจัยจากคะแนนของแบบสอบถามความพึงพอใจที่ให้ผู้เข้าร่วมการทดลองทำหลังการทดลองการพิสูจน์ตัวตนในครั้งที่ 3 ใช้เกณฑ์การแปลความหมายเพื่อจัดระดับคะแนนเฉลี่ยค่าความพึงพอใจ กำหนดเป็นช่วงคะแนน ดังต่อไปนี้

| | | | |
|---|---|---|---|
| คะแนนเฉลี่ย | 4.50 - 5.00 | แปลความว่า | มีความพึงพอใจมากที่สุด |
| คะแนนเฉลี่ย | 3.50 - 4.49 | แปลความว่า | มีความพึงพอใจมาก |
| คะแนนเฉลี่ย | 2.50 - 3.49 | แปลความว่า | มีความพึงพอใจปานกลาง |
| คะแนนเฉลี่ย | 1.50 - 2.49 | แปลความว่า | มีความพึงพอใจน้อย |
| คะแนนเฉลี่ย | 1.00 - 1.49 | แปลความว่า | มีความพึงพอใจน้อยที่สุด |

# บทที่ 4
# ผลการทดลอง

ในบทนี้จะนำเสนอผลการวิเคราะห์ข้อมูลที่ได้จากกลุ่มตัวอย่างเพื่อสรุปผลการทดลอง ประกอบไปด้วย ผลการวิเคราะห์ข้อมูลส่วนตัวของผู้เข้าร่วมการทดลอง ผลการวิเคราะห์ข้อมูลด้านการใช้งาน (Usability) ผลการวิเคราะห์ข้อมูลด้านความปลอดภัย (Security) ผลการวิเคราะห์ข้อมูลด้านความพึงพอใจ และผลการวิเคราะห์เพิ่มเติม ได้แก่ ผลการวิเคราะห์ความถี่ของรูปภาพที่ถูกเลือกใช้ และผลการวิเคราะห์ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้

## 4.1 ผลการวิเคราะห์ข้อมูลทั่วไปของผู้เข้าร่วมการทดลอง

จากผู้เข้าร่วมการทดลองจำนวน 60 คน เป็นเพศหญิง 45 คน คิดเป็นร้อยละ 75 เป็นเพศชาย 15 คน คิดเป็นร้อยละ 25 ส่วนใหญ่มีอายุอยู่ในช่วง 31-40 ปี 28 คน คิดเป็นร้อยละ 50 รองลงมาอายุ 21 - 30 ปี คิดเป็นร้อยละ 33.3 มีการศึกษาในระดับปริญญาตรี 28 คน คิดเป็นร้อยละ 46.7 ส่วนใหญ่หรือร้อยละ 76.7 มีความถี่ในการใช้งานคอมพิวเตอร์สัปดาห์ละ 4-6 วัน และผู้เข้าร่วมการทดลองเคยผ่านการพิสูจน์ตัวตนด้วยรหัสผ่านตัวอักษร รวมถึงเคยใช้งานควบคู่กับอุปกรณ์จำพวกการ์ด และการพิสูจน์ตัวตนโดยการใช้เอกลักษณ์เฉพาะบุคคลมาแล้วทุกคน และมีเพียง 1 คน ที่เคยใช้งานการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ ในส่วนการตั้งรหัสผ่านผู้เข้าร่วมการทดลองส่วนใหญ่ตั้งรหัสผ่านเหมือนกันทุกบัญชี ร้อยละ 41.7 และตั้งรหัสผ่านเหมือนกันบางบัญชี ร้อยละ 36.7 และส่วนใหญ่ใช้วิธีการเก็บรหัสผ่านโดยการจำ ร้อยละ 70 และใช้วิธีการจดบันทึก ร้อยละ 30

ตารางที่ 4.1

*จำนวนและค่าร้อยละของผู้เข้าร่วมการทดลอง จำแนกตามเพศ*

| เพศ | จำนวน (คน) | ร้อยละ (%) |
|---|---|---|
| ชาย | 15 | 25 |
| หญิง | 45 | 75 |
| รวม | 60 | 100 |

ตารางที่ 4.2

*จำนวนและค่าร้อยละของผู้เข้าร่วมการทดลอง จำแนกตามช่วงอายุ*

| ช่วงอายุ | จำนวน (คน) | ร้อยละ (%) |
|---|---|---|
| 21 - 30 ปี | 20 | 33.3 |
| 31 - 40 ปี | 30 | 50.0 |
| 41 - 50 ปี | 7 | 11.7 |
| 51 ปีขึ้นไป | 3 | 5.0 |
| รวม | 60 | 100.0 |

ตารางที่ 4.3

*จำนวนและร้อยละของผู้เข้าร่วมการทดลอง จำแนกตามระดับการศึกษา*

| ระดับการศึกษา | จำนวน (คน) | ร้อยละ (%) |
|---|---|---|
| ต่ำกว่าปริญญาตรี | 15 | 25 |
| ปริญญาตรี | 28 | 46.7 |
| สูงกว่าปริญญาตรี | 17 | 28.3 |
| รวม | 60 | 100.0 |

## 4.2 ผลการวิเคราะห์ผลการทดลองด้านการใช้งาน (Usability)

ผลการวิเคราะห์ผลการทดลองด้านการใช้งาน ประกอบไปด้วย จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน ของการทดลองทั้ง 3 ครั้ง ได้แก่ ครั้งที่ 1 หลังจากการลงทะเบียนทันที ครั้งที่ 2 หลังจากการลงทะเบียนไปแล้ว 3 วัน และครั้งที่ 3 หลังจากการลงทะเบียนไปแล้ว 15 วัน มีรายละเอียดดังนี้

### 4.2.1 ผลการทดลองครั้งที่ 1 หลังจากการลงทะเบียนทันที

เมื่อผู้เข้าร่วมการทดลองทำการลงทะเบียนเพื่อตั้งรหัสผ่านรูปภาพเสร็จ จะให้ทำการพิสูจน์ตัวตนทันที ซึ่งข้อมูลที่นำมาใช้ในการวิเคราะห์ ได้แก่ จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน ดังนี้

#### 4.2.1.1 จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน

การทดลองด้านการใช้งานจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง โดยโปรแกรมจะทำการบันทึกจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนตามที่ได้ทำการทดลอง

ตารางที่ 4.4

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 1.13 | 0.434 | 1 | 3 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 1.10 | 0.403 | 1 | 3 |
| รวม | 60 | 1.12 | 0.415 | 1 | 3 |

จากตารางที่ 4.4 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=1.10, S.D.=0.403) ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=1.13, S.D.=0.434)

ตารางที่ 4.5

*ค่าสถิติวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยจำนวนรอบในการตั้งรหัสผ่านระหว่างการตั้งรหัสผ่าน 1 รอบ กับการตั้งรหัสผ่าน 2 รอบ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 0.335 | 0.565 | 0.308 | 58 | 0.759 |

จากตารางที่ 4.5 ผลการวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ พบว่า กลุ่มทดลองทั้งสองกลุ่มมีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=0.308, P=0.759>0.05)

ตารางที่ 4.6

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 1.03 | 0.183 | 1 | 2 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 1.20 | 0.551 | 1 | 3 |
| รวม | 60 | 1.12 | 0.415 | 1 | 3 |

จากตารางที่ 4.6 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=1.03, S.D.=0.183) ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{x}$=1.20, S.D.=0.551)

ตารางที่ 4.7

*ค่าสถิติวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยการมีกฎในการเลือกรหัสผ่านระหว่างการมีกฎกับการไม่มีกฎ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 11.479 | 0.001 | -1.573 | 58 | 0.125 |

จากตารางที่ 4.7 ผลการวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับกลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท พบว่า กลุ่มทดลองทั้งสองกลุ่มมีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=-1.573, P=0.125>0.05)

ตารางที่ 4.8

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 1.07 | 0.258 | 1 | 2 |
| | ไม่มีกฎ | 15 | 1.20 | 0.561 | 1 | 3 |
| 2 รอบ | มีกฎ | 15 | 1.00 | 0.000 | 1 | 1 |
| | ไม่มีกฎ | 15 | 1.20 | 0.561 | 1 | 3 |
| รวม | | 60 | 1.12 | 0.415 | 1 | 3 |

จากตารางที่ 4.8 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=1.00, S.D.=0.000)

การวิเคราะห์สถิติจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) แตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=4.210, P=0.009<0.05) จึงใช้วิธีวิเคราะห์สถิติแบบทางเดียว (One-way ANOVA) ก็พบว่ามีค่าความแปรปรวนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=4.210, P=0.009<0.05) จึงต้องใช้วิธีการวิเคราะห์สถิติอ้างอิงแบบไม่มีพารามิเตอร์ (Non-parametric) ด้วยวิธี Kruskal-Wallis Test ดังนี้

ตารางที่ 4.9

*ค่าสถิติวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test*

| | Chi-Square | df | Asymp. Sig. |
|---|---|---|---|
| Kruskal-Wallis Test | 2.414 | 3 | 0.491 |

จากตารางที่ 4.9 ผลการวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test พบว่า กลุ่มทดลองทั้ง 4 กลุ่มมีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนไม่แตกต่างกัน (P=0.491>0.05)

**4.2.1.2 เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน**

การทดลองด้านการใช้งาน โปรแกรมจะเริ่มบันทึกเวลาที่ใช้ในการพิสูจน์เมื่อผู้เข้าร่วมการทดลองเข้าสู่หน้าจอการพิสูจน์ตัวตน จนกระทั้งผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนสำเร็จหรือทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง

ตารางที่ 4.10

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบ ในการตั้งรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 61.97 | 39.157 | 27 | 233 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 68.73 | 27.502 | 35 | 136 |
| รวม | 60 | 65.35 | 33.720 | 27 | 233 |

จากตารางที่ 4.10 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{X}$=61.97, S.D.= 39.157) ใช้เวลาในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ ($\bar{X}$=68.73, S.D.= 27.502)

ตารางที่ 4.11

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 64.30 | 21.032 | 33 | 117 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 66.40 | 43.228 | 27 | 233 |
| รวม | 60 | 65.35 | 33.720 | 27 | 233 |

จากตารางที่ 4.11 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=64.30, S.D.= 21.032) ใช้เวลาในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{x}$=66.40, S.D.= 43.228)

ตารางที่ 4.12

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 63.87 | 24.764 | 33 | 117 |
| | ไม่มีกฎ | 15 | 60.07 | 50.548 | 27 | 233 |
| 2 รอบ | มีกฎ | 15 | 64.73 | 17.396 | 39 | 105 |
| | ไม่มีกฎ | 15 | 72.73 | 35.068 | 35 | 136 |
| รวม | | 60 | 65.35 | 33.720 | 27 | 233 |

จากตารางที่ 4.12 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการ

เลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้เวลาในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=60.07, S.D.=50.548) และกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้เวลาในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=72.73, S.D.= 35.068)

การวิเคราะห์ความแปรปรวนของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่ามีค่าความแปรปรวน (Levene's Test) ไม่แตกต่างกัน (F=1.650, P=0.188>0.05)

ตารางที่ 4.13

*ค่าสถิติวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects)*

| ปัจจัยที่ศึกษา | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | 686.817 | 1 | 686.817 | 0.584 | 0.448 |
| กฎในการเลือกรหัสผ่าน | 66.150 | 1 | 66.150 | 0.056 | 0.813 |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | 522.150 | 1 | 522.150 | 0.444 | 0.508 |

จากตารางที่ 4.13 ผลการวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects) ด้วยวิธีวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการพิสูจน์ตัวตน (F=0.584, P=0.448>0.05) ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการพิสูจน์ตัวตน (F=0.056, P=0.813>0.05) และทั้งสองปัจจัยไม่มีอิทธิพลร่วมต่อเวลาที่ใช้ในการพิสูจน์ตัวตน (F=0.444, P=0.508>0.05)

#### 4.2.1.3 ความสำเร็จในการพิสูจน์ตัวตน

การทดลองด้านการใช้งานจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนสำเร็จในครั้งที่ 1 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 100 คะแนน หากสำเร็จในครั้งที่ 2 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 80 คะแนน หากสำเร็จในครั้งที่ 3 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 60 คะแนน หากสำเร็จ

ในครั้งที่ 4 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 40 คะแนน หากสำเร็จในครั้งที่ 5 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 20 คะแนน และไม่สำเร็จครบ 5 ครั้ง จะมีคะแนนเป็นศูนย์

ตารางที่ 4.14

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 97.33 | 8.683 | 60 | 100 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 98.00 | 8.052 | 60 | 100 |
| รวม | 60 | 97.67 | 8.309 | 60 | 100 |

จากตารางที่ 4.14 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{X}$=98.00, S.D.= 8.052) มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{X}$=97.33, S.D.= 8.683)

ตารางที่ 4.15

*ค่าสถิติวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยจำนวนรอบในการตั้งรหัสผ่านระหว่างการตั้งรหัสผ่าน 1 รอบ กับการตั้งรหัสผ่าน 2 รอบ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 0.335 | 0.565 | 0.308 | 58 | 0.759 |

จากตารางที่ 4.15 ผลการวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ พบว่า กลุ่มทดลองทั้งสองกลุ่มมีคะแนนความสำเร็จในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=0.308, P=0.759>0.05)

ตารางที่ 4.16

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 99.33 | 3.651 | 80 | 100 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 96.00 | 11.017 | 60 | 100 |
| รวม | 60 | 97.67 | 8.309 | 60 | 100 |

จากตารางที่ 4.16 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=99.33, S.D.= 3.651) มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{x}$=96.00, S.D.= 11.017)

ตารางที่ 4.17

*ค่าสถิติวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยการมีกฎในการเลือกรหัสผ่านระหว่างการมีกฎกับการไม่มีกฎ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 11.479 | 0.001 | -1.573 | 58 | 0.125 |

จากตารางที่ 4.17 ผลการวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับกลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท พบว่า กลุ่มทดลองทั้งสองกลุ่มมีคะแนนความสำเร็จในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=-1.573, P=0.125>0.05)

ตารางที่ 4.18

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 98.67 | 5.164 | 80 | 100 |
| | ไม่มีกฎ | 15 | 96.00 | 11.212 | 60 | 100 |
| 2 รอบ | มีกฎ | 15 | 100.00 | 0.000 | 100 | 100 |
| | ไม่มีกฎ | 15 | 96.00 | 11.212 | 60 | 100 |
| รวม | | 60 | 97.67 | 80309 | 60 | 100 |

จากตารางที่ 4.18 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=1.00, S.D.=0.000)

การวิเคราะห์สถิติของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) แตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=4.210, P=0.009<0.05) จึงใช้วิธีวิเคราะห์สถิติแบบทางเดียว (One-way ANOVA) ก็พบว่ามีค่าความแปรปรวนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=4.210, P=0.009<0.05) จึงต้องใช้วิธีการวิเคราะห์สถิติอ้างอิงแบบไม่มีพารามิเตอร์ (Non-parametric) ด้วยวิธี Kruskal-Wallis Test

ตารางที่ 4.19

*ค่าสถิติวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test*

| | Chi-Square | df | Asymp. Sig. |
|---|---|---|---|
| Kruskal-Wallis Test | 2.414 | 3 | 0.491 |

จากตารางที่ 4.19 ผลการวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test พบว่า กลุ่มทดลองทั้ง 4 กลุ่มมีคะแนนความสำเร็จในการพิสูจน์ตัวตนไม่แตกต่างกัน (P=0.491>0.05)

**4.2.1.4 เวลาเฉลี่ยที่ใช้ในการสร้างรหัสผ่าน**

โปรแกรมจะบันทึกเวลาที่ใช้ในการสร้างรหัสผ่านเมื่อผู้เข้าร่วมการทดลองเข้าสู่หน้าจอการลงทะเบียน จนกระทั่งผู้เข้าร่วมการทดลองทำการลงทะเบียนสำเร็จ

ตารางที่ 4.20

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการสร้างรหัสผ่าน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบ ในการตั้งรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 114.93 | 47.872 | 35 | 226 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 108.00 | 35.051 | 42 | 180 |
| รวม | 60 | 111.47 | 41.744 | 35 | 226 |

จากตารางที่ 4.20 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการสร้างรหัสผ่าน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=108.00, S.D.= 35.051) ใช้เวลาในการสร้างรหัสผ่านน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=114.93, S.D.= 47.872)

ตารางที่ 4.21

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการสร้างรหัสผ่าน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 106.80 | 43.941 | 36 | 226 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 116.13 | 39.614 | 35 | 212 |
| รวม | 60 | 111.47 | 41.744 | 35 | 226 |

จากตารางที่ 4.21 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการสร้างรหัสผ่าน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{X}$=106.80, S.D.= 43.941) ใช้เวลาในการสร้างรหัสผ่านน้อยกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{X}$=116.13, S.D.= 39.614)

ตารางที่ 4.22

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการสร้างรหัสผ่าน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 110.60 | 52.805 | 36 | 226 |
| | ไม่มีกฎ | 15 | 119.27 | 43.801 | 35 | 212 |
| 2 รอบ | มีกฎ | 15 | 103.00 | 34.353 | 49 | 180 |
| | ไม่มีกฎ | 15 | 113.00 | 36.210 | 42 | 178 |
| รวม | | 60 | 111.47 | 41.744 | 35 | 226 |

จากตารางที่ 4.22 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการสร้างรหัสผ่าน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน

พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้เวลาในการสร้างรหัสผ่านน้อยที่สุด ($\bar{x}$=103.00, S.D.= 34.353) และกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้เวลาในการสร้างรหัสผ่านมากที่สุด ($\bar{x}$=119.27, S.D.= 43.801)

การวิเคราะห์ความแปรปรวนของเวลาที่ใช้ในการสร้างรหัสผ่าน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่ามีค่าความแปรปรวน (Levene's Test) ไม่แตกต่างกัน (F=1.332, P=0.273>0.05)

ตารางที่ 4.23

*ค่าสถิติวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการสร้างรหัสผ่าน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects)*

| ปัจจัยที่ศึกษา | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | 721.067 | 1 | 721.067 | 0.401 | 0.529 |
| กฎในการเลือกรหัสผ่าน | 1306.667 | 1 | 1306.667 | 0.726 | 0.398 |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | 6.667 | 1 | 6.667 | 0.004 | 0.952 |

จากตารางที่ 4.23 ผลการวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการสร้างรหัสผ่าน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects) ด้วยวิธีวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการสร้างรหัสผ่าน (F=0.401, P=0.529>0.05) ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการสร้างรหัสผ่าน (F=0.726, P=0.398>0.05) และทั้งสองปัจจัยไม่มีอิทธิพลร่วมต่อเวลาที่ใช้ในการสร้างรหัสผ่าน (F=0.004, P=0.952>0.05)

#### 4.2.1.5 สรุปผลการทดลองด้านการใช้งาน ครั้งที่ 1

จากการวิเคราะห์ผลการทดลองด้านการใช้งานครั้งที่ 1 หลังจากการลงทะเบียนทันที ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน

สามารถสรุปผลการวิเคราะห์สถิติความแตกต่างได้ว่า จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน ความสำเร็จในการพิสูจน์ตัวตน และเวลาเฉลี่ยที่ใช้ในการสร้างรหัสผ่าน ในแต่ละกลุ่มทดลองไม่มีความแตกต่างกัน ดังตารางที่ 4.24

ตารางที่ 4.24

*สรุปผลการวิเคราะห์สถิติความแตกต่างของผลการทดลองด้านการใช้งานครั้งที่ 1*

| ปัจจัยที่ศึกษา | จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน | เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน | ความสำเร็จในการพิสูจน์ตัวตน | เวลาเฉลี่ยที่ใช้ในการสร้างรหัสผ่าน |
|---|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |
| กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |

### 4.2.2 ผลการทดลองครั้งที่ 2 หลังจากการลงทะเบียนไปแล้ว 3 วัน

เมื่อผู้เข้าร่วมการทดลองทำการลงทะเบียนเพื่อตั้งรหัสผ่านรูปภาพเสร็จ จะให้ทำการพิสูจน์ตัวตนอีกครั้งหลังจากการลงทะเบียนไปแล้ว 3 วัน ซึ่งข้อมูลที่นำมาใช้ในการวิเคราะห์ได้แก่ จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน มีรายละเอียดดังนี้

#### 4.2.2.1 จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน

การทดลองด้านการใช้งานจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง โดยโปรแกรมจะทำการบันทึกจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนตามที่ได้ทำการทดลอง

ตารางที่ 4.25

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 1.20 | 0.484 | 1 | 3 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 1.87 | 1.042 | 1 | 4 |
| รวม | 60 | 1.53 | 0.873 | 1 | 4 |

จากตารางที่ 4.25 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=1.20, S.D.=0.484) ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=1.87, S.D.=1.042)

ตารางที่ 4.26

*ค่าสถิติวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยจำนวนรอบในการตั้งรหัสผ่านระหว่างการตั้งรหัสผ่าน 1 รอบ กับการตั้งรหัสผ่าน 2 รอบ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 19.957 | 0.000 | -3.179 | 58 | 0.003* |

*ที่ระดับนัยสำคัญ 0.05.

จากตารางที่ 426. ผลการวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ พบว่า กลุ่มทดลองทั้งสองกลุ่มมีจำนวนครั้ง

ที่ใช้ในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (t=-3.179, P=0.003<0.05) โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ

ตารางที่ 4.27

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 1.50 | 0.820 | 1 | 4 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 1.57 | 0.935 | 1 | 4 |
| รวม | 60 | 1.53 | 0.873 | 1 | 4 |

จากตารางที่ 4.27 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=1.50, S.D.=0.820) ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{x}$=1.57, S.D.=0.935)

ตารางที่ 4.28

*ค่าสถิติวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยการมีกฎในการเลือกรหัสผ่านระหว่างการมีกฎกับการไม่มีกฎ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 0.477 | 0.492 | -0.294 | 58 | 0.770 |

จากตารางที่ 4.28 ผลการวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับกลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท พบว่า กลุ่มทดลองทั้งสองกลุ่มใช้จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=-0.294, P=0.770>0.05)

ตารางที่ 4.29

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 1.27 | 0.594 | 1 | 3 |
| | ไม่มีกฎ | 15 | 1.13 | 0.352 | 1 | 2 |
| 2 รอบ | มีกฎ | 15 | 1.73 | 0.961 | 1 | 4 |
| | ไม่มีกฎ | 15 | 2.00 | 1.134 | 1 | 4 |
| รวม | | 60 | 1.53 | 0.873 | 1 | 4 |

จากตารางที่ 4.29 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=1.13, S.D.=0.352) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=2.00, S.D.=1.134)

การวิเคราะห์สถิติของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) แตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=7.348, P=0.000<0.05) จึงใช้วิธีวิเคราะห์สถิติแบบทางเดียว (One-way ANOVA) ก็พบว่ามี

ค่าความแปรปรวนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=7.348, P=0.000<0.05) จึงต้องใช้วิธีการวิเคราะห์สถิติอ้างอิงแบบไม่มีพารามิเตอร์ (Non-parametric) ด้วยวิธี Kruskal-Wallis Test

ตารางที่ 4.30

*ค่าสถิติวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test*

| | Chi-Square | df | Asymp. Sig. |
|---|---|---|---|
| Kruskal-Wallis Test | 8.967 | 3 | 0.030* |

*ที่ระดับนัยสำคัญ 0.05

จากตารางที่ 4.30 ผลการวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test พบว่า กลุ่มทดลองทั้ง 4 กลุ่ม มีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (P=0.030<0.05) จึงต้องทำการวิเคราะห์เปรียบเทียบความแตกต่างเป็นรายคู่ด้วยวิธี Mann-Whitney U Test

ตารางที่ 4.31

*ค่าสถิติวิเคราะห์เปรียบเทียบความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Mann-Whitney U Test*

| กลุ่มทดลอง | เปรียบเทียบกับ กลุ่มทดลอง | Mann-Whitney U | Asymp. Sig. (2-tailed) |
|---|---|---|---|
| ใช้ 1 รอบ + มีกฎ | ใช้ 1 รอบ + ไม่มีกฎ | 104.000 | 0.586 |
| | ใช้ 2 รอบ + มีกฎ | 81.000 | 0.117 |
| | ใช้ 2 รอบ + ไม่มีกฎ | 70.500 | 0.043* |
| ใช้ 1 รอบ + ไม่มีกฎ | ใช้ 2 รอบ + มีกฎ | 72.000 | 0.037* |
| | ใช้ 2 รอบ + ไม่มีกฎ | 62.500 | 0.013* |
| ใช้ 2 รอบ + มีกฎ | ใช้ 2 รอบ + ไม่มีกฎ | 99.000 | 0.545 |

*ที่ระดับนัยสำคัญ 0.05

จากตารางที่ 4.31 ผลการวิเคราะห์เปรียบเทียบความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Mann-Whitney U Test โดยการเปรียบเทียบรายคู่ทีละคู่ พบว่า มีคู่ของกลุ่มทดลองที่ใช้จำนวนครั้งในการพิสูจน์ตัวตนแตกต่างกัน 3 คู่ ดังนี้

1. กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ ($P=0.043<0.05$) โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

2. กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ มีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ ($P=0.037<0.05$) โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ

3. กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ ($P=0.013<0.05$) โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

จากผลการวิเคราะห์เปรียบเทียบความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนเป็นรายคู่ทีละคู่ และพิจารณาค่าเฉลี่ยของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน พบว่า กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยที่สุด

#### 4.2.2.2 เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน

การทดลองด้านการใช้งาน โปรแกรมจะเริ่มบันทึกเวลาที่ใช้ในการพิสูจน์เมื่อผู้เข้าร่วมการทดลองเข้าสู่หน้าจอการพิสูจน์ตัวตน จนกระทั้งผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนสำเร็จหรือทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง

ตารางที่ 4.32

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบ ในการตั้งรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 89.07 | 49.230 | 37 | 204 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 97.63 | 54.044 | 41 | 236 |
| รวม | 60 | 93.35 | 51.435 | 37 | 236 |

จากตารางที่ 4.32 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=89.07, S.D.= 49.230) ใช้เวลาในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=97.63, S.D.= 54.044)

ตารางที่ 4.33

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 100.17 | 51.526 | 37 | 204 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 86.53 | 51.295 | 42 | 236 |
| รวม | 60 | 93.35 | 51.435 | 37 | 236 |

จากตารางที่ 4.33 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{x}$=86.53, S.D.= 51.295) ใช้เวลาในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=100.17, S.D.= 51.526)

ตารางที่ 4.34

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 100.87 | 58.586 | 37 | 204 |
| | ไม่มีกฎ | 15 | 77.27 | 35.912 | 42 | 141 |
| 2 รอบ | มีกฎ | 15 | 99.47 | 45.456 | 41 | 158 |
| | ไม่มีกฎ | 15 | 95.80 | 63.061 | 42 | 236 |
| รวม | | 60 | 93.35 | 51.435 | 37 | 236 |

จากตารางที่ 4.34 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้เวลาในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=77.27, S.D.= 35.912) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้เวลาในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=100.87, S.D.= 58.586)

การวิเคราะห์ความแปรปรวนของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่ามีค่าความแปรปรวน (Levene's Test) ไม่แตกต่างกัน (F=1.728, P=0.172>0.05)

ตารางที่ 4.35

*ค่าสถิติวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects)*

| ปัจจัยที่ศึกษา | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | 1100.817 | 1 | 1100.817 | 0.409 | 0.525 |
| กฎในการเลือกรหัสผ่าน | 2788.017 | 1 | 2788.017 | 1.036 | 0.313 |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | 1490.017 | 1 | 1490.017 | 0.554 | 0.460 |

จากตารางที่ 4.35 ผลการวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects) ด้วยวิธีวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการพิสูจน์ตัวตน (F=0.409, P=0.525>0.05) ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการพิสูจน์ตัวตน (F=1.036, P=0.313>0.05) และทั้งสองปัจจัยไม่มีอิทธิพลร่วมต่อเวลาที่ใช้ในการพิสูจน์ตัวตน (F=0.554, P=0.460>0.05)

**4.2.2.3 ความสำเร็จในการพิสูจน์ตัวตน**

การทดลองด้านการใช้งานจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนสำเร็จในครั้งที่ 1 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 100 คะแนน หากสำเร็จในครั้งที่ 2 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 80 คะแนน หากสำเร็จในครั้งที่ 3 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 60 คะแนน หากสำเร็จในครั้งที่ 4 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 40 คะแนน หากสำเร็จในครั้งที่ 5 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 20 คะแนน และไม่สำเร็จครบ 5 ครั้ง จะมีคะแนนเป็นศูนย์

ตารางที่ 4.36

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 96.00 | 9.685 | 60 | 100 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 82.67 | 20.833 | 40 | 100 |
| รวม | 60 | 89.33 | 17.454 | 40 | 100 |

จากตารางที่ 4.36 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{X}$=96.00, S.D.= 9.685) มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{X}$=82.67, S.D.=20.833)

ตารางที่ 4.37

*ค่าสถิติวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยจำนวนรอบในการตั้งรหัสผ่านระหว่างการตั้งรหัสผ่าน 1 รอบ กับการตั้งรหัสผ่าน 2 รอบ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 19.957 | 0.000 | 3.179 | 58 | 0.003* |

*ที่ระดับนัยสำคัญ 0.05.

จากตารางที่ 4.37 ผลการวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับกลุ่ม

ทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ พบว่า กลุ่มทดลองทั้งสองกลุ่มมีคะแนนความสำเร็จในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (t=-3.179, P=0.003<0.05) โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ

ตารางที่ 4.38

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 90.00 | 16.400 | 40 | 100 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 88.67 | 18.705 | 40 | 100 |
| รวม | 60 | 89.33 | 17.454 | 40 | 100 |

จากตารางที่ 4.38 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=90.00, S.D.=16.400) มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{x}$=88.67, S.D.= 18.705)

ตารางที่ 4.39

*ค่าสถิติวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยการมีกฎในการเลือกรหัสผ่านระหว่างการมีกฎกับการไม่มีกฎ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 0.477 | 0.492 | 0.294 | 58 | 0.770 |

จากตารางที่ 4.39 ผลการวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับกลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท พบว่า กลุ่มทดลองทั้งสองกลุ่มมีคะแนนความสำเร็จในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=0.294, P=0.770>0.05)

ตารางที่ 4.40

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 94.67 | 11.872 | 60 | 100 |
| | ไม่มีกฎ | 15 | 97.33 | 7.037 | 80 | 100 |
| 2 รอบ | มีกฎ | 15 | 85.33 | 19.223 | 40 | 100 |
| | ไม่มีกฎ | 15 | 80.00 | 22.678 | 40 | 100 |
| รวม | | 60 | 89.33 | 17.454 | 40 | 100 |

จากตารางที่ 4.40 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=97.33, S.D.= 7.037)

การวิเคราะห์สถิติของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) แตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=7.348, P=0.000<0.05) จึงใช้วิธีวิเคราะห์สถิติแบบทางเดียว (One-way ANOVA) ก็พบว่ามีค่าความแปรปรวนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=7.348, P=0.000<0.05) จึงต้องใช้วิธีการวิเคราะห์สถิติอ้างอิงแบบไม่มีพารามิเตอร์ (Non-parametric) ด้วยวิธี Kruskal-Wallis Test

ตารางที่ 4.41

*ค่าสถิติวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test*

| | Chi-Square | df | Asymp. Sig. |
|---|---|---|---|
| Kruskal-Wallis Test | 8.967 | 3 | 0.030* |

*ที่ระดับนัยสำคัญ 0.05

จากตารางที่ 4.41 ผลการวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test พบว่า กลุ่มทดลองทั้ง 4 กลุ่ม มีคะแนนความสำเร็จในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (P=0.030<0.05) จึงต้องทำการวิเคราะห์เปรียบเทียบความแตกต่างเป็นรายคู่ด้วยวิธี Mann-Whitney U Test

ตารางที่ 4.42

*ค่าสถิติวิเคราะห์เปรียบเทียบความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Mann-Whitney U Test*

| กลุ่มทดลอง | เปรียบเทียบกับ กลุ่มทดลอง | Mann-Whitney U | Asymp. Sig. (2-tailed) |
|---|---|---|---|
| ใช้ 1 รอบ + มีกฎ | ใช้ 1 รอบ + ไม่มีกฎ | 104.000 | 0.586 |
| | ใช้ 2 รอบ + มีกฎ | 81.000 | 0.117 |
| | ใช้ 2 รอบ + ไม่มีกฎ | 70.500 | 0.043* |
| ใช้ 1 รอบ + ไม่มีกฎ | ใช้ 2 รอบ + มีกฎ | 72.000 | 0.037* |
| | ใช้ 2 รอบ + ไม่มีกฎ | 62.500 | 0.013* |
| ใช้ 2 รอบ + มีกฎ | ใช้ 2 รอบ + ไม่มีกฎ | 99.000 | 0.545 |

*ที่ระดับนัยสำคัญ 0.05

จากตารางที่ 4.42 ผลการวิเคราะห์เปรียบเทียบความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Mann-Whitney U Test โดยการเปรียบเทียบรายคู่ทีละคู่ พบว่า มีคู่ของกลุ่มทดลองที่มีคะแนนความสำเร็จในการพิสูจน์ตัวตนแตกต่างกัน 3 คู่ ดังนี้

1. กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ ($P=0.043<0.05$) โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

2. กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ มีคะแนนความสำเร็จในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ ($P=0.037<0.05$) โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ

3. กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ ($P=0.013<0.05$) โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

จากผลการวิเคราะห์เปรียบเทียบความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน เป็นรายคู่ทีละคู่ และพิจารณาค่าเฉลี่ยของคะแนนความสำเร็จในการพิสูจน์ตัวตน พบว่า กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด

#### 4.2.1.4 สรุปผลการทดลองด้านการใช้งาน ครั้งที่ 2

จากการวิเคราะห์ผลการทดลองด้านการใช้งานครั้งที่ 2 หลังจากการลงทะเบียนไปแล้ว 3 วัน ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน สามารถสรุปผลการวิเคราะห์สถิติความแตกต่างได้ว่า จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนและความสำเร็จในการพิสูจน์ตัวตนในแต่ละกลุ่มทดลองมีความแตกต่างกัน โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนน้อยที่สุดและมีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด ส่วนเวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตนในแต่ละกลุ่มทดลองไม่มีความแตกต่างกัน ดังตารางที่ 4.43

ตารางที่ 4.43

*สรุปผลการวิเคราะห์สถิติความแตกต่างของผลการทดลองด้านการใช้งานครั้งที่ 2*

| ปัจจัยที่ศึกษา | จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน | เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน | ความสำเร็จในการพิสูจน์ตัวตน |
|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | แตกต่าง | ไม่แตกต่าง | แตกต่าง |
| กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | แตกต่าง | ไม่แตกต่าง | แตกต่าง |

### 4.2.3 ผลการทดลองครั้งที่ 3 หลังจากการลงทะเบียนไปแล้ว 15 วัน

เมื่อผู้เข้าร่วมการทดลองทำการลงทะเบียนเพื่อตั้งรหัสผ่านรูปภาพเสร็จ จะให้ทำการพิสูจน์ตัวตนอีกครั้งหลังจากการลงทะเบียนไปแล้ว 15 วัน ซึ่งข้อมูลที่นำมาใช้ในการวิเคราะห์ได้แก่ จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน มีรายละเอียดดังนี้

#### 4.2.3.1 จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน

การทดลองด้านการใช้งาน จะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง โดยโปรแกรมจะทำการบันทึกจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนตามที่ได้ทำการทดลอง

ตารางที่ 4.44

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 1.40 | 0.894 | 1 | 5 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 2.00 | 1.597 | 1 | 5 |
| รวม | 60 | 1.70 | 1.319 | 1 | 5 |

จากตารางที่ 4.44 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=1.40, S.D.=0.894) ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=2.00, S.D.=1.597)

ตารางที่ 4.45

*ค่าสถิติวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยจำนวนรอบในการตั้งรหัสผ่านระหว่างการตั้งรหัสผ่าน 1 รอบ กับการตั้งรหัสผ่าน 2 รอบ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 13.843 | 0.000 | -1.795 | 58 | 0.079 |

จากตารางที่ 4.45 ผลการวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ พบว่า กลุ่มทดลองทั้งสองกลุ่มมีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=-1.795, P=0.079>0.05)

ตารางที่ 4.46

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 1.67 | 1.124 | 1 | 5 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 1.73 | 1.507 | 1 | 5 |
| รวม | 60 | 1.70 | 1.319 | 1 | 5 |

จากตารางที่ 4.46 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=1.67, S.D.=1.124) ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{x}$=1.73, S.D.=1.507)

ตารางที่ 4.47

*ค่าสถิติวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยการมีกฎในการเลือกรหัสผ่านระหว่างการมีกฎกับการไม่มีกฎ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 2.362 | 0.130 | -0.194 | 58 | 0.847 |

จากตารางที่ 4.47 ผลการวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับกลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท พบว่า กลุ่มทดลองทั้งสองกลุ่มใช้จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=-0.194, P=0.847>0.05)

ตารางที่ 4.48

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 1.53 | 0.743 | 1 | 3 |
| | ไม่มีกฎ | 15 | 1.27 | 1.033 | 1 | 5 |
| 2 รอบ | มีกฎ | 15 | 1.80 | 1.424 | 1 | 5 |
| | ไม่มีกฎ | 15 | 2.20 | 1.781 | 1 | 5 |
| รวม | | 60 | 1.70 | 1.319 | 1 | 5 |

จากตารางที่ 4.48 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=1.27, S.D.=1.033) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=2.20, S.D.=1.781)

การวิเคราะห์สถิติของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) แตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=6.844, P=0.001<0.05) จึงใช้วิธีวิเคราะห์สถิติแบบทางเดียว (One-way ANOVA) ก็พบว่ามีค่าความแปรปรวนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=6.844, P=0.001<0.05) จึงต้องใช้วิธีการวิเคราะห์สถิติอ้างอิงแบบไม่มีพารามิเตอร์ (Non-parametric) ด้วยวิธี Kruskal-Wallis Test

ตารางที่ 4.49

*ค่าสถิติวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test*

| | Chi-Square | df | Asymp. Sig. |
|---|---|---|---|
| Kruskal-Wallis Test | 3.991 | 3 | 0.262 |

จากตารางที่ 4.49 ผลการวิเคราะห์ความแตกต่างของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test พบว่า กลุ่มทดลองทั้ง 4 กลุ่มมีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนไม่แตกต่างกัน (P=0.262>0.05)

**4.2.3.2 เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน**

การทดลองด้านการใช้งาน โปรแกรมจะเริ่มบันทึกเวลาที่ใช้ในการพิสูจน์เมื่อผู้เข้าร่วมการทดลองเข้าสู่หน้าจอการพิสูจน์ตัวตน จนกระทั้งผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนสำเร็จหรือทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง

ตารางที่ 4.50

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบ ในการตั้งรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 93.57 | 52.507 | 48 | 243 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 100.93 | 68.917 | 37 | 362 |
| รวม | 60 | 97.25 | 60.856 | 37 | 362 |

จากตารางที่ 4.50 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=93.57, S.D.= 52.507) ใช้เวลาในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=100.93, S.D.= 68.917)

ตารางที่ 4.51

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 96.30 | 49.309 | 38 | 205 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 98.20 | 71.424 | 37 | 362 |
| รวม | 60 | 97.25 | 60.856 | 37 | 362 |

จากตารางที่ 4.51 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=96.30, S.D.= 49.309) ใช้เวลาในการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{x}$=98.20,S.D.= 71.424)

ตารางที่ 4.52

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 102.60 | 56.414 | 48 | 205 |
| | ไม่มีกฎ | 15 | 84.53 | 48.513 | 48 | 243 |
| 2 รอบ | มีกฎ | 15 | 90.00 | 42.058 | 38 | 190 |
| | ไม่มีกฎ | 15 | 111.87 | 88.393 | 37 | 362 |
| รวม | | 60 | 97.25 | 60.856 | 37 | 362 |

จากตารางที่ 4.52 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการ

เลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้เวลาในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=84.53, S.D.= 48.513) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้เวลาในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=111.87, S.D.= 88.393)

การวิเคราะห์ความแปรปรวนของเวลาที่ใช้ในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่ามีค่าความแปรปรวน (Levene's Test) ไม่แตกต่างกัน (F=1.341, P=0.270>0.05)

ตารางที่ 4.53

*ค่าสถิติวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects)*

| ปัจจัยการทดลอง | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | 814.017 | 1 | 814.017 | 0.215 | 0.644 |
| กฎในการเลือกรหัสผ่าน | 54.150 | 1 | 54.150 | 0.014 | 0.905 |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | 5980.017 | 1 | 5980.017 | 1.582 | 0.214 |

จากตารางที่ 4.53 ผลการวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่าน กับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects) ด้วยวิธีวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการพิสูจน์ตัวตน (F=0.215, P=0.644>0.05) ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการพิสูจน์ตัวตน (F=0.014, P=0.905>0.05) และทั้งสองปัจจัยไม่มีอิทธิพลร่วมต่อเวลาที่ใช้ในการพิสูจน์ตัวตน (F=1.582, P=0.214>0.05)

**4.2.3.3 ความสำเร็จในการพิสูจน์ตัวตน**

การทดลองด้านการใช้งานจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนสำเร็จในครั้งที่ 1 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 100 คะแนน หากสำเร็จในครั้งที่ 2 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 80 คะแนน หากสำเร็จในครั้งที่ 3 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 60 คะแนน หากสำเร็จ

ในครั้งที่ 4 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 40 คะแนน หากสำเร็จในครั้งที่ 5 จะได้คะแนนการพิสูจน์ตัวตนสำเร็จ 20 คะแนน และไม่สำเร็จครบ 5 ครั้ง จะมีคะแนนเป็นศูนย์

ตารางที่ 4.54

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 91.33 | 20.800 | 0 | 100 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 77.33 | 37.410 | 0 | 100 |
| รวม | 60 | 84.33 | 30.828 | 0 | 100 |

จากตารางที่ 4.54 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=91.33, S.D.= 20.800) มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=77.33, S.D.= 37.410)

ตารางที่ 4.55

*ค่าสถิติวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยจำนวนรอบในการตั้งรหัสผ่านระหว่างการตั้งรหัสผ่าน 1 รอบ กับการตั้งรหัสผ่าน 2 รอบ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 13.143 | 0.001 | 1.791 | 58 | 0.78 |

จากตารางที่ 4.55 ผลการวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ กับกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ พบว่า กลุ่มทดลองทั้งสองกลุ่มมีคะแนนความสำเร็จในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=1.791, P=0.78>0.05)

ตารางที่ 4.56

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 86.00 | 24.719 | 0 | 100 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 82.67 | 36.287 | 0 | 100 |
| รวม | 60 | 84.33 | 30.828 | 0 | 100 |

จากตารางที่ 4.56 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=86.00, S.D.=24.719) มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ($\bar{x}$=82.67, S.D.= 36.287)

ตารางที่ 4.57

*ค่าสถิติวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test*

| เปรียบเทียบปัจจัยการมีกฎในการเลือกรหัสผ่านระหว่างการมีกฎกับการไม่มีกฎ | Levene's Test for Equality of Variances | | t-test for Equality of Means | | |
|---|---|---|---|---|---|
| | F | Sig. | t | df | Sig. (2-tailed) |
| Equal variances assumed | 3.718 | 0.59 | 0.416 | 58 | 0.679 |

จากตารางที่ 4.57 ผลการวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน โดยวิธีการวิเคราะห์สถิติแบบ Independent-Samples T Test ระหว่างกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ กับกลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท พบว่า กลุ่มทดลองทั้งสองกลุ่มมีคะแนนความสำเร็จในการพิสูจน์ตัวตนไม่แตกต่างกัน (t=-0.416, P=0.679>0.05)

ตารางที่ 4.58

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 89.33 | 14.864 | 60 | 100 |
| | ไม่มีกฎ | 15 | 93.33 | 25.820 | 0 | 100 |
| 2 รอบ | มีกฎ | 15 | 82.67 | 31.952 | 0 | 100 |
| | ไม่มีกฎ | 15 | 72.00 | 42.628 | 0 | 100 |
| รวม | | 60 | 84.33 | 30.828 | 0 | 100 |

จากตารางที่ 4.58 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=93.33, S.D.= 25.820) และ ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=72.00, S.D.= 42.628)

การวิเคราะห์สถิติของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) แตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=6.233, P=0.001<0.05) จึงใช้วิธีวิเคราะห์สถิติแบบทางเดียว (One-way ANOVA) ก็พบว่ามี

ค่าความแปรปรวนแตกต่างกันอย่างมีนัยสำคัญทางสถิติ (F=6.233, P=0.001<0.05) จึงต้องใช้วิธีการวิเคราะห์สถิติอ้างอิงแบบไม่มีพารามิเตอร์ (Non-parametric) ด้วยวิธี Kruskal-Wallis Test

ตารางที่ 4.59

*ค่าสถิติวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test*

| | Chi-Square | df | Asymp. Sig. |
|---|---|---|---|
| Kruskal-Wallis Test | 3.973 | 3 | 0.264 |

จากตารางที่ 4.59 ผลการวิเคราะห์ความแตกต่างของคะแนนความสำเร็จในการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธี Kruskal-Wallis Test พบว่า กลุ่มทดลองทั้ง 4 กลุ่มมีคะแนนความสำเร็จในการพิสูจน์ตัวตนไม่แตกต่างกัน (P=0.264>0.05)

**4.2.3.4 สรุปผลการทดลองด้านการใช้งาน ครั้งที่ 3**

จากการวิเคราะห์ผลการทดลองด้านการใช้งานครั้งที่ 3 หลังจากการลงทะเบียนไปแล้ว 15 วัน ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน สามารถสรุปผลการวิเคราะห์สถิติความแตกต่างได้ว่า จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน ในแต่ละกลุ่มทดลองไม่มีความแตกต่างกัน ดังตารางที่ 4.60

ตารางที่ 4.60

*สรุปผลการวิเคราะห์สถิติความแตกต่างของผลการทดลองด้านการใช้งานครั้งที่ 3*

| ปัจจัยที่ศึกษา | จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน | เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน | ความสำเร็จในการพิสูจน์ตัวตน |
|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |
| กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |

### 4.2.4 สรุปผลการวิเคราะห์ผลการทดลองด้านการใช้งาน (Usability)

ผลการวิเคราะห์ผลการทดลองด้านการใช้งาน ประกอบไปด้วย จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน ของการทดลองทั้ง 3 ครั้ง ได้แก่ ครั้งที่ 1 หลังจากการลงทะเบียนทันที ครั้งที่ 2 หลังจากการลงทะเบียนไปแล้ว 3 วัน และครั้งที่ 3 หลังจากการลงทะเบียนไปแล้ว 15 วัน นั้น พบว่า กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนน้อยที่สุด มีเวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตนน้อยที่สุด และมีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด โดยมีรายละเอียดดังนี้

ตารางที่ 4.61

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | | ครั้งที่ 1 | ครั้งที่ 2 | ครั้งที่ 3 | ค่าเฉลี่ย |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | ค่า | | | | |
| 1 รอบ | มีกฎ | $\bar{x}$ | 1.07 | 1.27 | 1.53 | 1.29 |
| | | S.D. | 0.258 | 0.594 | 0.743 | 0.589 |
| | ไม่มีกฎ | $\bar{x}$ | 1.20 | 1.13 | 1.27 | 1.20 |
| | | S.D. | 0.561 | 0.352 | 1.033 | 0.694 |
| 2 รอบ | มีกฎ | $\bar{x}$ | 1.00 | 1.73 | 1.80 | 1.51 |
| | | S.D. | 0.000 | 0.961 | 1.424 | 1.036 |
| | ไม่มีกฎ | $\bar{x}$ | 1.20 | 2.00 | 2.20 | 1.80 |
| | | S.D. | 0.561 | 1.134 | 1.781 | 1.307 |

จากตารางที่ 4.61 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=1.20, S.D.=0.694) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ

2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=1.80, S.D.=1.307)

ตารางที่ 4.62

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | | ครั้งที่ 1 | ครั้งที่ 2 | ครั้งที่ 3 | ค่าเฉลี่ย |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | ค่า | | | | |
| 1 รอบ | มีกฎ | $\bar{x}$ | 63.87 | 110.60 | 100.87 | 91.78 |
| | | S.D. | 24.764 | 52.805 | 58.586 | 51.247 |
| | ไม่มีกฎ | $\bar{x}$ | 60.07 | 119.27 | 77.27 | 85.54 |
| | | S.D. | 50.548 | 43.801 | 35.912 | 45.605 |
| 2 รอบ | มีกฎ | $\bar{x}$ | 64.73 | 103.00 | 99.47 | 89.07 |
| | | S.D. | 17.396 | 34.353 | 45.456 | 39.197 |
| | ไม่มีกฎ | $\bar{x}$ | 72.73 | 113.00 | 95.80 | 93.84 |
| | | S.D. | 35.068 | 36.210 | 63.061 | 66.381 |

จากตารางที่ 4.62 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้เวลาเฉลี่ยในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=85.54, S.D.=45.605) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้เวลาเฉลี่ยในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=93.84, S.D.=66.381)

ตารางที่ 4.63

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | | ครั้งที่ 1 | ครั้งที่ 2 | ครั้งที่ 3 | ค่าเฉลี่ย |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | ค่า | | | | |
| 1 รอบ | มีกฎ | $\bar{x}$ | 98.67 | 94.67 | 89.33 | 94.22 |
| | | S.D. | 5.164 | 11.872 | 14.864 | 11.772 |
| | ไม่มีกฎ | $\bar{x}$ | 96.00 | 97.33 | 93.33 | 95.55 |
| | | S.D. | 11.212 | 7.037 | 25.820 | 16.453 |
| 2 รอบ | มีกฎ | $\bar{x}$ | 100.00 | 85.33 | 82.67 | 89.33 |
| | | S.D. | 0.000 | 19.223 | 31.952 | 22.401 |
| | ไม่มีกฎ | $\bar{x}$ | 96.00 | 80.00 | 72.00 | 82.67 |
| | | S.D. | 11.212 | 22.678 | 42.628 | 29.726 |

จากตารางที่ 4.63 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=95.55, S.D.= 16.453) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีคะแนนความสำเร็จในการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=82.67, S.D.= 29.726)

**4.3 ผลการวิเคราะห์ผลการทดลองด้านความปลอดภัย (Security)**

ผลการวิเคราะห์ผลการทดลองด้านความปลอดภัย ประกอบไปด้วย จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน ของการทดลองทั้ง 3 ครั้ง ได้แก่ ครั้งที่ 1 ทดลองการโจรกรรมการพิสูจน์ตัวตนหลังจากการลงทะเบียนทันที ครั้งที่ 2 ทดลองการโจรกรรมการพิสูจน์ตัวตนหลังจากการ

ลงทะเบียนไปแล้ว 3 วัน ครั้งที่ 3 ทดลองการโจรกรรมการพิสูจน์ตัวตนหลังจากการลงทะเบียนไปแล้ว 15 วัน มีรายละเอียดดังนี้

**4.3.1 ผลการทดลองการโจรกรรมครั้งที่ 1 หลังจากการลงทะเบียนทันที**

เมื่อผู้เข้าร่วมการทดลองด้านการใช้งานทำการพิสูจน์ตัวตนเสร็จสิ้น จะให้ผู้เข้าร่วมการทดลองที่รับหน้าที่ทำการโจรกรรมการพิสูจน์ตัวตนทำการโจรกรรมการพิสูจน์ตัวตนทันที ซึ่งข้อมูลที่นำมาใช้ในการวิเคราะห์ ได้แก่ จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน ดังนี้

**4.3.1.1 จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน**

ให้ผู้เข้าร่วมการทดลองที่รับหน้าที่ทำการโจรกรรมการพิสูจน์ตัวตนใช้วิธีการแอบมอง (Shoulder surfing) โดยพยายามแอบมองในขณะที่ผู้เข้าร่วมการทดลองด้านการใช้งานกำลังทำการพิสูจน์ตัวตน และให้นำรหัสผ่านที่โจรกรรมได้มาทำการพิสูจน์ตัวตน โดยให้โอกาสทำการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากทำการโจรกรรมการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง โดยโปรแกรมจะทำการบันทึกจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนตามที่ได้ทำการทดลอง

ตารางที่ 4.64

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| | ไม่มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| 2 รอบ | มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| | ไม่มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| รวม | | 60 | 5.00 | 0.000 | 5 | 5 |

จากตารางที่ 4.64 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการ

เลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่ม มีค่าเฉลี่ยของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนเท่ากัน ($\bar{x}$=5.00, S.D.=0.000)

**4.3.1.2 เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน**

การทดลองด้านความปลอดภัย โปรแกรมจะเริ่มบันทึกเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนเมื่อผู้เข้าร่วมการทดลองเข้าสู่หน้าจอการพิสูจน์ตัวตน จนกระทั้งผู้เข้าร่วมการทดลองทำการโจรกรรมการพิสูจน์ตัวตนสำเร็จ หรือทำการโจรกรรมการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง

ตารางที่ 4.65

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 206.77 | 41.932 | 150 | 342 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 147.93 | 34.691 | 74 | 239 |
| รวม | 60 | 177.35 | 48.330 | 74 | 342 |

จากตารางที่ 4.65 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=206.77, S.D.=41.932) ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=147.93, S.D.=34.691)

ตารางที่ 4.66

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 174.40 | 49.693 | 74 | 342 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 180.30 | 47.589 | 105 | 333 |
| รวม | 60 | 177.35 | 48.330 | 74 | 342 |

จากตารางที่ 4.66 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=174.40, S.D.=49.693) ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท ($\bar{x}$=180.30, S.D.= 47.589)

ตารางที่ 4.67

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 205.47 | 43.626 | 150 | 342 |
| | ไม่มีกฎ | 15 | 208.07 | 41.658 | 153 | 333 |
| 2 รอบ | มีกฎ | 15 | 143.33 | 33.820 | 74 | 177 |
| | ไม่มีกฎ | 15 | 152.53 | 36.107 | 105 | 239 |
| รวม | | 60 | 177.35 | 48.330 | 74 | 342 |

จากตารางที่ 4.67 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการ

เลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=143.33, S.D.= 33.820) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=208.07, S.D.= 41.658)

การวิเคราะห์สถิติของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) ไม่แตกต่างกัน (F=0.019, P=0.996>0.05)

ตารางที่ 4.68

*ค่าสถิติวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects)*

| ปัจจัยที่ศึกษา | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | 51920.417 | 1 | 51920.417 | 34.124 | 0.000* |
| กฎในการเลือกรหัสผ่าน | 522.150 | 1 | 522.150 | 0.343 | 0.560 |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | 163.350 | 1 | 163.350 | 0.107 | 0.744 |

*ที่ระดับนัยสำคัญ 0.05

จากตารางที่ 4.68 ผลการวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่าน กับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects) ด้วยวิธีวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านมีอิทธิพลต่อเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนอย่างมีนัยสำคัญทางสถิติ (F=34.124, P=0.000<0.05) ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน (F=0.343, P=0.560>0.05) และทั้งสองปัจจัยไม่มีอิทธิพลร่วมต่อเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน (F=0.107, P=0.744>0.05)

#### 4.3.1.3 ความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน

การทดลองด้านความปลอดภัยจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการโจรกรรมการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากผู้เข้าร่วมการทดลองทำการโจรกรรมการพิสูจน์ตัวตนสำเร็จในครั้งที่ 1 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 100 คะแนน หากสำเร็จในครั้งที่ 2 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 80 คะแนน หากสำเร็จในครั้งที่ 3 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 60 คะแนน หากสำเร็จในครั้งที่ 4 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 40 คะแนน หากสำเร็จในครั้งที่ 5 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 20 คะแนน และไม่สำเร็จครบ 5 ครั้ง จะมีคะแนนเป็นศูนย์

ตารางที่ 4.69

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| | ไม่มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| 2 รอบ | มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| | ไม่มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| รวม | | 60 | 0.00 | 0.000 | 0 | 0 |

จากตารางที่ 4.69 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่มไม่สามารถทำการโจรกรรมการพิสูจน์ตัวตนได้สำเร็จ

#### 4.3.1.4 สรุปผลการทดลองการโจรกรรมครั้งที่ 1

จากการวิเคราะห์ผลการทดลองการโจรกรรมครั้งที่ 1 หลังจากการลงทะเบียนทันที ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่มไม่สามารถทำการโจรกรรมการพิสูจน์ตัวตนได้สำเร็จ โดยสามารถสรุปผลการวิเคราะห์สถิติความแตกต่างได้ว่า เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านมีความแตกต่างกัน โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้ง

รหัสผ่านรูปภาพ 1 รอบ ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ส่วนจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน ในแต่ละกลุ่มทดลองไม่มีความแตกต่างกัน ดังตารางที่ 4.70

ตารางที่ 4.70

*สรุปผลการวิเคราะห์สถิติความแตกต่างของผลการทดลองการโจรกรรมครั้งที่ 1*

| ปัจจัยที่ศึกษา | จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน | เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน | ความสำเร็จในการพิสูจน์ตัวตน |
|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | ไม่แตกต่าง | แตกต่าง | ไม่แตกต่าง |
| กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |

### 4.3.2 ผลการทดลองการโจรกรรมครั้งที่ 2 หลังจากการลงทะเบียน 3 วัน

เมื่อผู้เข้าร่วมการทดลองด้านการใช้งานทำการพิสูจน์ตัวตนเสร็จสิ้น จะให้ผู้เข้าร่วมการทดลองที่รับหน้าที่ทำการโจรกรรมการพิสูจน์ตัวตนทำการโจรกรรมการพิสูจน์ตัวตนทันที ซึ่งข้อมูลที่นำมาใช้ในการวิเคราะห์ ได้แก่ จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน ดังนี้

#### 4.3.2.1 จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน

ให้ผู้เข้าร่วมการทดลองที่รับหน้าที่ทำการโจรกรรมการพิสูจน์ตัวตนใช้วิธีการแอบมอง (Shoulder surfing) โดยพยายามแอบมองในขณะที่ผู้เข้าร่วมการทดลองด้านการใช้งานกำลังทำการพิสูจน์ตัวตน และให้นำรหัสผ่านที่โจรกรรมได้มาทำการพิสูจน์ตัวตน โดยให้โอกาสทำการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากทำการโจรกรรมการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง โดยโปรแกรมจะทำการบันทึกจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนตามที่ได้ทำการทดลอง

ตารางที่ 4.71

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| | ไม่มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| 2 รอบ | มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| | ไม่มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| รวม | | 60 | 5.00 | 0.000 | 5 | 5 |

จากตารางที่ 4.71 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่ม มีค่าเฉลี่ยของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนเท่ากัน ($\bar{X}$=5.00, S.D.=0.000)

**4.3.2.2 เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน**

การทดลองด้านความปลอดภัย โปรแกรมจะเริ่มบันทึกเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนเมื่อผู้เข้าร่วมการทดลองเข้าสู่หน้าจอการพิสูจน์ตัวตน จนกระทั่งผู้เข้าร่วมการทดลองทำการโจรกรรมการพิสูจน์ตัวตนสำเร็จหรือทำการโจรกรรมการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง

ตารางที่ 4.72

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 195.43 | 36.225 | 140 | 285 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 148.13 | 31.663 | 82 | 236 |
| รวม | 60 | 171.78 | 41.311 | 82 | 285 |

จากตารางที่ 4.72 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=195.43, S.D.=36.225) ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=148.13, S.D.=31.663)

ตารางที่ 4.73

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 169.07 | 38.070 | 93 | 272 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 174.50 | 44.804 | 82 | 285 |
| รวม | 60 | 171.78 | 41.311 | 82 | 285 |

จากตารางที่ 4.73 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=169.07, S.D.=38.070) ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนน้อยกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท ($\bar{x}$=174.50, S.D.=44.804)

ตารางที่ 4.74

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 198.80 | 26.458 | 155 | 272 |
| | ไม่มีกฎ | 15 | 192.07 | 44.653 | 140 | 285 |
| 2 รอบ | มีกฎ | 15 | 139.33 | 20.191 | 93 | 164 |
| | ไม่มีกฎ | 15 | 156.93 | 38.769 | 82 | 236 |
| รวม | | 60 | 171.78 | 41.311 | 82 | 285 |

จากตารางที่ 4.74 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนน้อยที่สุด ($\bar{X}$=139.33, S.D.= 20.191) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากที่สุด ($\bar{X}$=198.80, S.D.= 26.458)

การวิเคราะห์สถิติของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) ไม่แตกต่างกัน (F=2.435, P=0.074>0.05)

ตารางที่ 4.75

*ค่าสถิติวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects)*

| ปัจจัยที่ศึกษา | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | 33559.350 | 1 | 33559.350 | 29.152 | 0.000* |
| กฎในการเลือกรหัสผ่าน | 442.817 | 1 | 442.817 | 0.385 | 0.538 |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | 2220.417 | 1 | 2220.417 | 1.929 | 0.170 |

*ที่ระดับนัยสำคัญ 0.05

จากตารางที่ 4.75 ผลการวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects) ด้วยวิธีวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านมีอิทธิพลต่อเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนอย่างมีนัยสำคัญทางสถิติ ($F=29.152$, $P=0.000<0.05$) ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ($F=0.385$, $P=0.538>0.05$) และทั้งสองปัจจัยไม่มีอิทธิพลร่วมต่อเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ($F=1.929$, $P=0.170>0.05$)

**4.3.2.3 ความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน**

การทดลองด้านความปลอดภัยจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการโจรกรรมการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากผู้เข้าร่วมการทดลองทำการโจรกรรมการพิสูจน์ตัวตนสำเร็จในครั้งที่ 1 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 100 คะแนน หากสำเร็จในครั้งที่ 2 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 80 คะแนน หากสำเร็จในครั้งที่ 3 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 60 คะแนน หากสำเร็จในครั้งที่ 4 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 40 คะแนน หากสำเร็จในครั้งที่ 5 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 20 คะแนน และไม่สำเร็จครบ 5 ครั้ง จะมีคะแนนเป็นศูนย์

ตารางที่ 4.76

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| | ไม่มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| 2 รอบ | มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| | ไม่มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| รวม | | 60 | 0.00 | 0.000 | 0 | 0 |

จากตารางที่ 4.76 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่มไม่สามารถทำการโจรกรรมการพิสูจน์ตัวตนได้สำเร็จ

#### 4.3.2.4 สรุปผลการทดลองการโจรกรรมครั้งที่ 2

จากการวิเคราะห์ผลการทดลองการโจรกรรมครั้งที่ 2 หลังจากการลงทะเบียน 3 วัน ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่มไม่สามารถทำการโจรกรรมการพิสูจน์ตัวตนได้สำเร็จ โดยสามารถสรุปผลการวิเคราะห์สถิติความแตกต่างได้ว่า เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านมีความแตกต่างกัน โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ส่วนจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน ในแต่ละกลุ่มทดลองไม่มีความแตกต่างกัน ดังตารางที่ 4.77

ตารางที่ 4.77

*สรุปผลการวิเคราะห์สถิติความแตกต่างของผลการทดลองการโจรกรรมครั้งที่ 2*

| ปัจจัยที่ศึกษา | จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน | เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน | ความสำเร็จในการพิสูจน์ตัวตน |
|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | ไม่แตกต่าง | แตกต่าง | ไม่แตกต่าง |
| กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |

**4.3.3 ผลการทดลองการโจรกรรมครั้งที่ 3 หลังจากการลงทะเบียน 15 วัน**

เมื่อผู้เข้าร่วมการทดลองด้านการใช้งานทำการพิสูจน์ตัวตนเสร็จสิ้น จะให้ผู้เข้าร่วมการทดลองที่รับหน้าที่ทำการโจรกรรมการพิสูจน์ตัวตนทำการโจรกรรมการพิสูจน์ตัวตนทันที ซึ่งข้อมูลที่นำมาใช้ในการวิเคราะห์ ได้แก่ จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน ดังนี้

**4.3.3.1 จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน**

ให้ผู้เข้าร่วมการทดลองที่รับหน้าที่ทำการโจรกรรมการพิสูจน์ตัวตนใช้วิธีการแอบมอง (Shoulder surfing) โดยพยายามแอบมองในขณะที่ผู้เข้าร่วมการทดลองด้านการใช้งานกำลังทำการพิสูจน์ตัวตน และให้นำรหัสผ่านที่โจรกรรมได้มาทำการพิสูจน์ตัวตน โดยให้โอกาสทำการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากทำการโจรกรรมการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง ถือว่าสิ้นสุดการทดลอง โดยโปรแกรมจะทำการบันทึกจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนตามที่ได้ทำการทดลอง

ตารางที่ 4.78

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ครั้ง) | Std. Deviation | Minimum (ครั้ง) | Maximum (ครั้ง) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| | ไม่มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| 2 รอบ | มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| | ไม่มีกฎ | 15 | 5.00 | 0.000 | 5 | 5 |
| รวม | | 60 | 5.00 | 0.000 | 5 | 5 |

จากตารางที่ 4.78 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่ม มีค่าเฉลี่ยของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนเท่ากัน ($\bar{X}$=5.00, S.D.=0.000)

**4.3.3.2 เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน**

การทดลองด้านความปลอดภัย โปรแกรมจะเริ่มบันทึกเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนเมื่อผู้เข้าร่วมการทดลองเข้าสู่หน้าจอการพิสูจน์ตัวตน จนกระทั่งผู้เข้าร่วมการทดลองทำการโจรกรรมการพิสูจน์ตัวตนสำเร็จหรือทำการโจรกรรมการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง

ตารางที่ 4.79

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน*

| ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| ตั้งรหัสผ่าน 1 รอบ | 30 | 180.63 | 35.008 | 100 | 265 |
| ตั้งรหัสผ่าน 2 รอบ | 30 | 146.90 | 33.456 | 63 | 191 |
| รวม | 60 | 163.77 | 37.972 | 63 | 265 |

จากตารางที่ 4.79 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ($\bar{x}$=180.63, S.D.=35.008) ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ($\bar{x}$=146.90, S.D.=33.456)

ตารางที่ 4.80

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยการมีกฎ ในการเลือกรหัสผ่าน | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|
| เลือกประเภทละ 2 รูปภาพ | 30 | 165.87 | 44.269 | 63 | 265 |
| ไม่มีกฎในการเลือกรูปภาพ | 30 | 161.67 | 31.058 | 77 | 243 |
| รวม | 60 | 163.77 | 37.972 | 63 | 265 |

จากตารางที่ 4.80 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่มีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ($\bar{x}$=165.87, S.D.=44.269) ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท ($\bar{x}$=161.67, S.D.=31.058)

ตารางที่ 4.81

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (วินาที) | Std. Deviation | Minimum (วินาที) | Maximum (วินาที) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 187.00 | 41.433 | 100 | 265 |
| | ไม่มีกฎ | 15 | 174.27 | 27.112 | 138 | 243 |
| 2 รอบ | มีกฎ | 15 | 144.73 | 37.226 | 63 | 191 |
| | ไม่มีกฎ | 15 | 149.07 | 30.377 | 77 | 189 |
| รวม | | 60 | 163.77 | 37.972 | 63 | 265 |

จากตารางที่ 4.81 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=144.73, S.D.=37.226) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=187.00, S.D.= 41.433)

การวิเคราะห์สถิติของเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) ไม่แตกต่างกัน (F=0.648, P=0.587>0.05)

ตารางที่ 4.82

*ค่าสถิติวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects)*

| ปัจจัยที่ศึกษา | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | 17069.067 | 1 | 17069.067 | 14.343 | 0.000* |
| กฎในการเลือกรหัสผ่าน | 264.600 | 1 | 264.600 | 0.222 | 0.639 |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | 1092.267 | 1 | 1092.267 | 0.918 | 0.342 |

*ที่ระดับนัยสำคัญ 0.05

จากตารางที่ 4.82 ผลการวิเคราะห์อิทธิพลร่วม (Interaction) เวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่านกับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects) ด้วยวิธีวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านมีอิทธิพลต่อเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนอย่างมีนัยสำคัญทางสถิติ ($F=14.343$, $P=0.000<0.05$) ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่มีอิทธิพลต่อเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ($F=0.222$, $P=0.639>0.05$) และทั้งสองปัจจัยไม่มีอิทธิพลร่วมต่อเวลาที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ($F=0.918$, $P=0.342>0.05$)

**4.3.3.3 ความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน**

การทดลองด้านความปลอดภัยจะกำหนดให้ผู้เข้าร่วมการทดลองมีโอกาสในการโจรกรรมการพิสูจน์ตัวตนได้ทั้งหมด 5 ครั้ง ซึ่งหากผู้เข้าร่วมการทดลองทำการโจรกรรมการพิสูจน์ตัวตนสำเร็จในครั้งที่ 1 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 100 คะแนน หากสำเร็จในครั้งที่ 2 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 80 คะแนน หากสำเร็จในครั้งที่ 3 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 60 คะแนน หากสำเร็จในครั้งที่ 4 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 40 คะแนน หากสำเร็จในครั้งที่ 5 จะได้คะแนนการโจรกรรมการพิสูจน์ตัวตนสำเร็จ 20 คะแนน และไม่สำเร็จครบ 5 ครั้ง จะมีคะแนนเป็นศูนย์

ตารางที่ 4.83

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (ร้อยละ) | Std. Deviation | Minimum (ร้อยละ) | Maximum (ร้อยละ) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| | ไม่มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| 2 รอบ | มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| | ไม่มีกฎ | 15 | 0.00 | 0.000 | 0 | 0 |
| รวม | | 60 | 0.00 | 0.000 | 0 | 0 |

จากตารางที่ 4.83 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่มไม่สามารถทำการโจรกรรมการพิสูจน์ตัวตนได้สำเร็จ

**4.3.3.4 สรุปผลการทดลองการโจรกรรมครั้งที่ 3**

จากการวิเคราะห์ผลการทดลองการโจรกรรมครั้งที่ 3 หลังจากการลงทะเบียน 15 วัน ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่ม ไม่สามารถทำการโจรกรรมการพิสูจน์ตัวตนได้สำเร็จ โดยสามารถสรุปผลการวิเคราะห์สถิติความแตกต่างได้ว่า เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน ตามปัจจัยจำนวนรอบในการตั้งรหัสผ่านมีความแตกต่างกัน โดยกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ใช้เวลาในการโจรกรรมการพิสูจน์ตัวตนมากกว่ากลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ส่วนจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน ในแต่ละกลุ่มทดลองไม่มีความแตกต่างกัน ดังตารางที่ 4.84

ตารางที่ 4.84

*สรุปผลการวิเคราะห์สถิติความแตกต่างของผลการทดลองการโจรกรรมครั้งที่ 3*

| ปัจจัยที่ศึกษา | จำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน | เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน | ความสำเร็จในการพิสูจน์ตัวตน |
|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | ไม่แตกต่าง | แตกต่าง | ไม่แตกต่าง |
| กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | ไม่แตกต่าง | ไม่แตกต่าง | ไม่แตกต่าง |

### 4.3.4 สรุปผลการวิเคราะห์ผลการทดลองด้านความปลอดภัย (Security)

ผลการวิเคราะห์ผลการทดลองด้านความปลอดภัย ประกอบไปด้วย จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน ของการทดลองทั้ง 3 ครั้ง ได้แก่ ครั้งที่ 1 ทดลองการโจรกรรมการพิสูจน์ตัวตนหลังจากลงทะเบียนทันที ครั้งที่ 2 ทดลองการโจรกรรมการพิสูจน์ตัวตนหลังจากลงทะเบียน 3 วัน ครั้งที่ 3 ทดลองการโจรกรรมการพิสูจน์ตัวตนหลังจากลงทะเบียน 15 วัน นั้น พบว่า ผลการทดลองด้านความปลอดภัย ไม่มีผู้เข้าร่วมการทดลองที่ทำการโจรกรรมการพิสูจน์ตัวตนได้ได้สำเร็จ ซึ่งแสดงว่า การทดลองทั้ง 4 กลุ่มทดลองมีความปลอดภัยจากการโจรกรรมการพิสูจน์ตัวตนด้วยวิธีการแอบมอง (Shoulder surfing) 100 เปอร์เซ็นต์ โดยมีรายละเอียดดังนี้

ตารางที่ 4.85

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | | ครั้งที่ 1 | ครั้งที่ 2 | ครั้งที่ 3 | ค่าเฉลี่ย |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | ค่า | | | | |
| 1 รอบ | มีกฎ | $\bar{x}$ | 5.00 | 5.00 | 5.00 | 5.00 |
| | | S.D. | 0.000 | 0.000 | 0.000 | 0.000 |
| | ไม่มีกฎ | $\bar{x}$ | 5.00 | 5.00 | 5.00 | 5.00 |
| | | S.D. | 0.000 | 0.000 | 0.000 | 0.000 |
| 2 รอบ | มีกฎ | $\bar{x}$ | 5.00 | 5.00 | 5.00 | 5.00 |
| | | S.D. | 0.000 | 0.000 | 0.000 | 0.000 |
| | ไม่มีกฎ | $\bar{x}$ | 5.00 | 5.00 | 5.00 | 5.00 |
| | | S.D. | 0.000 | 0.000 | 0.000 | 0.000 |

จากตารางที่ 4.85 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของจำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่ม มีค่าเฉลี่ยจำนวนครั้งในการโจรกรรมการพิสูจน์ตัวตนเท่ากัน ($\bar{x}$=5.00, S.D.= 0.000)

ตารางที่ 4.86

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | | ครั้งที่ 1 | ครั้งที่ 2 | ครั้งที่ 3 | ค่าเฉลี่ย |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | ค่า | | | | |
| 1 รอบ | มีกฎ | $\bar{x}$ | 205.47 | 198.80 | 187.00 | 197.09 |
| | | S.D. | 43.626 | 26.458 | 41.433 | 37.870 |
| | ไม่มีกฎ | $\bar{x}$ | 208.07 | 192.07 | 174.27 | 191.47 |
| | | S.D. | 41.658 | 44.653 | 27.112 | 40.192 |
| 2 รอบ | มีกฎ | $\bar{x}$ | 143.33 | 139.33 | 144.73 | 142.46 |
| | | S.D. | 33.820 | 20.191 | 37.226 | 30.658 |
| | ไม่มีกฎ | $\bar{x}$ | 152.53 | 156.93 | 149.07 | 152.84 |
| | | S.D. | 36.107 | 38.769 | 30.377 | 34.602 |

จากตารางที่ 4.86 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของเวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า ค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้เวลาเฉลี่ยในการโจรกรรมการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=197.09, S.D.=37.870) และค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ ใช้เวลาเฉลี่ยในการโจรกรรมการพิสูจน์ตัวตนน้อยที่สุด ($\bar{x}$=142.46, S.D.=30.658)

ตารางที่ 4.87

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการโจรกรรมการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | | ครั้งที่ 1 | ครั้งที่ 2 | ครั้งที่ 3 | ค่าเฉลี่ย |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | ค่า | | | | |
| 1 รอบ | มีกฎ | $\bar{x}$ | 0.00 | 0.00 | 0.00 | 0.00 |
| | | S.D. | 0.000 | 0.000 | 0.000 | 0.000 |
| | ไม่มีกฎ | $\bar{x}$ | 0.00 | 0.00 | 0.00 | 0.00 |
| | | S.D. | 0.000 | 0.000 | 0.000 | 0.000 |
| 2 รอบ | มีกฎ | $\bar{x}$ | 0.00 | 0.00 | 0.00 | 0.00 |
| | | S.D. | 0.000 | 0.000 | 0.000 | 0.000 |
| | ไม่มีกฎ | $\bar{x}$ | 0.00 | 0.00 | 0.00 | 0.00 |
| | | S.D. | 0.000 | 0.000 | 0.000 | 0.000 |

จากตารางที่ 4.87 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความสำเร็จในการโจรกรรมการพิสูจน์ตัวตนทั้ง 3 ครั้ง จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่า กลุ่มทดลองทั้ง 4 กลุ่ม มีค่าเฉลี่ยของคะแนนความสำเร็จในการโจรกรรมการพิสูจน์ตัวตนเท่ากัน ($\bar{x}$=0.00, S.D.= 0.000)

## 4.4 ผลการวิเคราะห์ข้อมูลด้านความพึงพอใจ

งานวิจัยนี้ใช้แบบสอบถามความพึงพอใจ เพื่อประเมินความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อโปรแกรมการพิสูจน์ตัวตนที่ออกแบบ โดยแบบสอบถามความพึงพอใจมีทั้งหมด 11 ข้อ ใช้แบบสอบถามแบบมาตราส่วนประมาณค่า (Rating scale) โดยแบ่งระดับคะแนนความพึงพอใจเป็น 5 ระดับ ผลการวิเคราะห์ดังต่อไปนี้

### 4.4.1 ผลการวิเคราะห์แบบสอบถามความพึงพอใจ

ตารางที่ 4.88

*แสดงค่าเฉลี่ยความถี่ ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความความพึงพอใจ จำแนกตามรายข้อของแบบสอบถามความพึงพอใจ*

| ข้อ | รายละเอียด | จำนวนครั้งที่ถูกเลือก (%) | | | | | Mean | S.D. |
|---|---|---|---|---|---|---|---|---|
| | | ระดับคะแนน | | | | | | |
| | | 1 | 2 | 3 | 4 | 5 | | |
| 1 | การสร้างรหัสผ่านในขั้นตอนการลงทะเบียนทำได้ง่าย | 1.7 | 3.3 | 15.0 | 43.3 | 36.7 | 4.10 | 0.896 |
| 2 | การเลือกรหัสผ่านทำได้ง่าย | 0.0 | 3.3 | 13.3 | 50.0 | 33.3 | 4.13 | 0.769 |
| 3 | รหัสผ่านรูปภาพทำให้สามารถจดจำได้ง่าย | 1.7 | 5.0 | 10.0 | 36.7 | 46.7 | 4.22 | 0.940 |
| 4 | ขั้นตอนในการลงทะเบียนและการเข้าสู่ระบบง่าย ไม่ซับซ้อน | 0.0 | 3.3 | 16.7 | 46.7 | 33.3 | 4.10 | 0.796 |
| 5 | ขั้นตอนการทำงานรวดเร็ว | 0.0 | 3.3 | 5.0 | 41.7 | 50.0 | 4.38 | 0.739 |
| 6 | ความพึงพอใจต่อรูปภาพ มีความคมชัดมีเอกลักษณ์ | 0.0 | 1.7 | 8.3 | 43.3 | 46.7 | 4.35 | 0.709 |
| 7 | ความพึงพอใจต่อส่วนต่อประสาน | 0.0 | 1.7 | 8.3 | 53.3 | 36.7 | 4.25 | 0.680 |
| 8 | โปรแกรมง่ายต่อการเข้าใจ | 0.0 | 3.3 | 13.3 | 45.0 | 38.3 | 4.18 | 0.792 |
| 9 | คุณคิดว่าวิธีการนี้มีความน่าเชื่อถือสามารถนำไปใช้งานได้จริง | 1.7 | 1.7 | 6.7 | 58.3 | 31.7 | 4.17 | 0.763 |
| 10 | ในด้านความปลอดภัย คุณคิดว่าวิธีการนี้มีความความปลอดภัย | 0.0 | 3.3 | 8.3 | 48.3 | 40.0 | 4.25 | 0.751 |
| 11 | ในด้านการใช้งาน คุณคิดว่าวิธีการนี้ใช้งานง่าย | 0.0 | 1.7 | 11.7 | 48.3 | 38.3 | 4.23 | 0.722 |
| รวม | | 0.46 | 2.87 | 10.60 | 46.81 | 39.26 | 4.21 | 0.780 |

จากตารางที่ 4.88 แสดงค่าเฉลี่ยความถี่ ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความความพึงพอใจ จำแนกตามรายข้อของแบบสอบถามความพึงพอใจ พบว่า ค่าเฉลี่ยความพึงพอใจต่อระบบการพิสูจน์ตัวตนที่ได้ออกแบบโดยรวมอยู่ในระดับพึงพอใจมาก ($\bar{x}$=4.21, S.D.=0.780)

### 4.4.2 สรุปผลการวิเคราะห์ด้านความพึงพอใจ

ตารางที่ 4.89

*ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความความพึงพอ จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน*

| ปัจจัยที่ศึกษา | | N | Mean (คะแนน) | Std. Deviation | Minimum (คะแนน) | Maximum (คะแนน) |
|---|---|---|---|---|---|---|
| จำนวนรอบ | กฎการเลือก | | | | | |
| 1 รอบ | มีกฎ | 15 | 4.19 | 0.458 | 3.55 | 5.00 |
| | ไม่มีกฎ | 15 | 4.30 | 0.655 | 2.55 | 5.00 |
| | รวม | 30 | 4.25 | 0.558 | 2.55 | 5.00 |
| 2 รอบ | มีกฎ | 15 | 4.18 | 0.609 | 3.00 | 5.00 |
| | ไม่มีกฎ | 15 | 4.18 | 0.690 | 2.00 | 5.00 |
| | รวม | 30 | 4.18 | 0.640 | 2.00 | 5.00 |
| รวม | มีกฎ | 30 | 4.19 | 0.530 | 3.00 | 5.00 |
| | ไม่มีกฎ | 30 | 4.24 | 0.664 | 2.00 | 5.00 |
| รวม | | 60 | 4.21 | 0.596 | 2.00 | 5.00 |

จากตารางที่ 4.89 แสดงค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของคะแนนความความพึงพอ จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน พบว่าค่าเฉลี่ยของกลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท มีความพึงพอใจต่อระบบการพิสูจน์ตัวตนมากที่สุด ($\bar{x}$=4.30, S.D.=0.655)

การวิเคราะห์สถิติของค่าเฉลี่ยคะแนนความความพึงพอ จำแนกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน ด้วยวิธีการวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่ามีค่าความแปรปรวน (Levene's Test) ไม่แตกต่างกัน (F=0.361, P=0.781>0.05)

ตารางที่ 4.90

*ค่าสถิติวิเคราะห์อิทธิพลร่วม (Interaction) ค่าเฉลี่ยคะแนนความความพึงพอ ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่าน กับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects)*

| ปัจจัยที่ศึกษา | Type III Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|
| จำนวนรอบในการตั้งรหัสผ่าน | 0.67 | 1 | 0.67 | 0.179 | 0.674 |
| กฎในการเลือกรหัสผ่าน | 0.45 | 1 | 0.45 | 0.120 | 0.730 |
| จำนวนรอบในการตั้งรหัสผ่าน * กฎในการเลือกรหัสผ่าน | 0.45 | 1 | 0.45 | 0.120 | 0.730 |

จากตารางที่ 4.90 ค่าสถิติวิเคราะห์อิทธิพลร่วม (Interaction) ค่าเฉลี่ยคะแนนความความพึงพอ ระหว่างปัจจัยจำนวนรอบในการตั้งรหัสผ่าน กับปัจจัยการมีกฎในการเลือกรหัสผ่าน (Tests of Between-Subjects Effects) ด้วยวิธีวิเคราะห์สถิติแบบสองทาง (Two-way ANOVA) พบว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านไม่มีอิทธิพลต่อความความพึงพอ (F=0.179, P=0.674>0.05) ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่มีอิทธิพลต่อความความพึงพอ (F=0.120, P=0.730>0.05) และทั้งสองปัจจัยไม่มีอิทธิพลร่วมต่อความความพึงพอ (F=0.120, P=0.730>0.05)

## 4.5 ผลการวิเคราะห์เพิ่มเติม

ผลการวิเคราะห์ผลเพิ่มเติม ประกอบไปด้วย ผลการวิเคราะห์ความเป็นไปได้ทั้งหมดของรหัสผ่าน ผลการวิเคราะห์ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่าน และผลการวิเคราะห์ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ มีรายละเอียดดังนี้

### 4.5.1 ผลการวิเคราะห์ความเป็นไปได้ทั้งหมดของรหัสผ่าน

การวิเคราะห์ความเป็นไปได้ทั้งหมดของรหัสผ่าน (Password space) สำหรับการตั้งรหัสผ่านรูปภาพจากตัวเลือกรูปภาพ 36 รูปภาพ เลือก 8 รูปภาพเป็นรหัสผ่าน โดยแยกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน คำนวณด้วยวิธีเรียงสับเปลี่ยน (Permutation) ดังนี้

กรณีที่ 1 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ

$$P_{n,r} = \frac{n!}{(n-r)!}$$

$$= \frac{9!}{(9-2)!}$$

$$= 72$$

เลือกรูปภาพ 4 ประเภท $= 72 \times 72 \times 72 \times 72$

$$= 26{,}873{,}856$$

จากการคำนวณด้วยวิธีเรียงสับเปลี่ยน (Permutation) จะได้ความเป็นไปได้ของรหัสผ่านทั้งหมด 26,873,856 วิธี

กรณีที่ 2 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ และไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

$$P_{n,r} = \frac{n!}{(n-r)!}$$

$$= \frac{36!}{(36-8)!}$$

$$= 1{,}220{,}096{,}908{,}800$$

จากการคำนวณด้วยวิธีเรียงสับเปลี่ยน (Permutation) จะได้ความเป็นไปได้ของรหัสผ่านทั้งหมด 1,220,096,908,800 วิธี

กรณีที่ 3 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ และมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ

รอบที่ 1

$$P_{n,r} = \frac{n!}{(n-r)!}$$

$$= \frac{9!}{(9-2)!}$$

$$= 72$$

เลือกรูปภาพ 2 ประเภท = 72 x 72

= 5,184

รอบที่ 2

$$P_{n,r} = \frac{n!}{(n-r)!}$$

$$= \frac{9!}{(9-2)!}$$

= 72

เลือกรูปภาพ 2 ประเภท = 72 x 72

= 5,184

รวม 2 รอบ = 5,184 + 5,184

= 10,368

จากการคำนวณด้วยวิธีเรียงสับเปลี่ยน (Permutation) จะได้ความเป็นไปได้ของรหัสผ่านทั้งหมด 10,368 วิธี

กรณีที่ 4 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ และไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท

รอบที่ 1

$$P_{n,r} = \frac{n!}{(n-r)!}$$

$$= \frac{18!}{(18-4)!}$$

= 73,440

รอบที่ 2

$$P_{n,r} = \frac{n!}{(n-r)!}$$

$$= \frac{18!}{(18-4)!}$$

= 73,440

รวม 2 รอบ = 73,440 + 73,440

= 146,880

จากการคำนวณด้วยวิธีเรียงสับเปลี่ยน (Permutation) จะได้ความเป็นไปได้ของรหัสผ่านทั้งหมด 146,880 วิธี

**4.5.2 ผลการวิเคราะห์ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่าน**

การทดลองการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยในขั้นตอนการลงทะเบียนจะให้ผู้เข้าร่วมการทดลองทำการเลือกรูปภาพจำนวน 8 รูปภาพ เพื่อตั้งเป็นรหัสผ่าน จากรูปภาพที่มีให้เลือกทั้งหมด 36 รูปภาพ จากการทดลองสามารถสรุปผลการวิเคราะห์ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่าน ได้ดังนี้

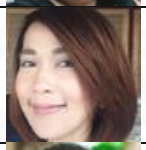
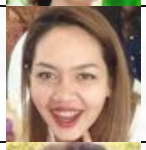
ตารางที่ 4.91

*ความถี่ของรูปภาพใบหน้าผู้ชายที่ถูกเลือกใช้เป็นรหัสผ่าน*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 1 |  | 22 | 4.58 |
| 2 |  | 18 | 3.75 |
| 3 |  | 16 | 3.33 |
| 4 |  | 16 | 3.33 |
| 5 |  | 13 | 2.71 |
| 6 |  | 13 | 2.71 |
| 7 |  | 12 | 2.50 |
| 8 |  | 8 | 1.67 |
| 9 |  | 4 | 0.83 |

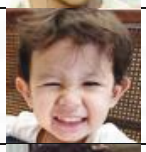
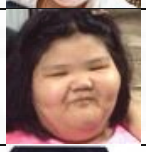
ตารางที่ 4.92

*ความถี่ของรูปภาพใบหน้าผู้หญิงที่ถูกเลือกใช้เป็นรหัสผ่าน*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 1 |  | 21 | 4.38 |
| 2 |  | 19 | 3.96 |
| 3 |  | 15 | 3.13 |
| 4 |  | 14 | 2.92 |
| 5 |  | 12 | 2.50 |
| 6 |  | 10 | 2.08 |
| 7 |  | 9 | 1.88 |
| 8 |  | 8 | 1.67 |
| 9 |  | 7 | 1.46 |

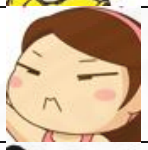
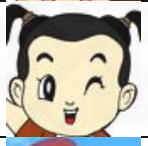
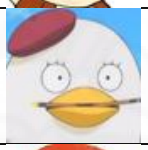
ตารางที่ 4.93

*ความถี่ของรูปภาพใบหน้าเด็กที่ถูกเลือกใช้เป็นรหัสผ่าน*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 1 |  | 24 | 5.00 |
| 2 |  | 19 | 3.96 |
| 3 |  | 17 | 3.54 |
| 4 |  | 15 | 3.13 |
| 5 |  | 13 | 2.71 |
| 6 |  | 11 | 2.29 |
| 7 |  | 10 | 2.08 |
| 8 |  | 9 | 1.88 |
| 9 |  | 6 | 1.25 |

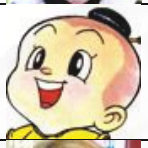
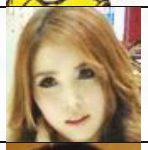
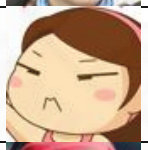
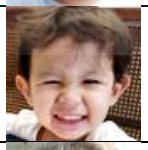
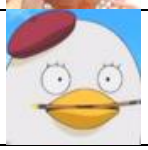
ตารางที่ 4.94

*ความถี่ของรูปภาพใบหน้าการ์ตูนที่ถูกเลือกใช้เป็นรหัสผ่าน*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 1 |  | 22 | 4.58 |
| 2 |  | 17 | 3.54 |
| 3 |  | 16 | 3.33 |
| 4 |  | 14 | 2.92 |
| 5 |  | 14 | 2.92 |
| 6 |  | 12 | 2.50 |
| 7 |  | 10 | 2.08 |
| 8 |  | 8 | 1.67 |
| 9 |  | 6 | 1.25 |

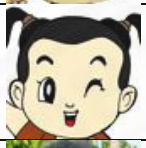
ตารางที่ 4.95

*ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่านแบบมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 1 |  | 14 | 5.83 |
| 2 |  | 13 | 5.42 |
| 3 |  | 13 | 5.42 |
| 4 |  | 12 | 5.00 |
| 5 |  | 11 | 4.58 |
| 6 |  | 10 | 4.17 |
| 7 |  | 10 | 4.17 |
| 8 |  | 9 | 3.75 |
| 9 |  | 9 | 3.75 |
| 10 |  | 8 | 3.33 |

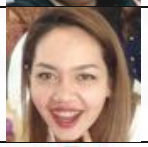
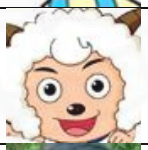
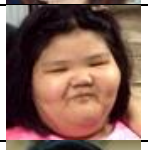
ตารางที่ 4.95 (ต่อ)

*ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่านแบบมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 11 |  | 8 | 3.33 |
| 12 |  | 8 | 3.33 |
| 13 |  | 8 | 3.33 |
| 14 |  | 7 | 2.92 |
| 15 |  | 6 | 2.50 |
| 16 |  | 6 | 2.50 |
| 17 |  | 6 | 2.50 |
| 18 |  | 6 | 2.50 |
| 19 |  | 6 | 2.50 |
| 20 |  | 6 | 2.50 |

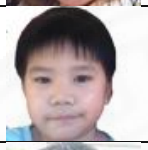
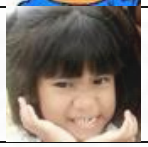
ตารางที่ 4.95 (ต่อ)

*ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่านแบบมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 21 |  | 6 | 2.50 |
| 22 |  | 6 | 2.50 |
| 23 |  | 6 | 2.50 |
| 24 |  | 5 | 2.08 |
| 25 |  | 5 | 2.08 |
| 26 |  | 5 | 2.08 |
| 27 |  | 5 | 2.08 |
| 28 |  | 5 | 2.08 |
| 29 |  | 4 | 1.67 |
| 30 |  | 4 | 1.67 |

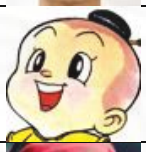
ตารางที่ 4.95 (ต่อ)

*ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่านแบบมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 31 |  | 4 | 1.67 |
| 32 |  | 3 | 1.25 |
| 33 |  | 3 | 1.25 |
| 34 |  | 2 | 0.83 |
| 35 |  | 1 | 0.42 |
| 36 |  | 0 | 0.00 |

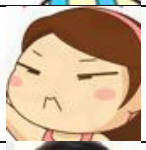
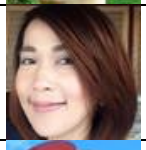
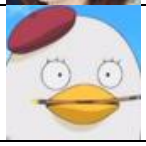
ตารางที่ 4.96

*ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่านแบบไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 1 |  | 12 | 5.00 |
| 2 |  | 10 | 4.17 |
| 3 |  | 10 | 4.17 |
| 4 |  | 10 | 4.17 |
| 5 |  | 9 | 3.75 |
| 6 |  | 9 | 3.75 |
| 7 |  | 9 | 3.75 |
| 8 |  | 9 | 3.75 |
| 9 |  | 9 | 3.75 |
| 10 |  | 9 | 3.75 |

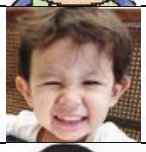
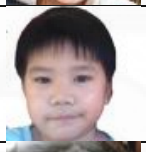
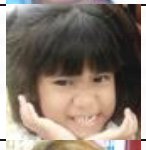
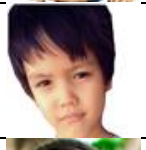
ตารางที่ 4.96 (ต่อ)

*ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่านแบบไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 11 |  | 8 | 3.33 |
| 12 |  | 8 | 3.33 |
| 13 |  | 7 | 2.92 |
| 14 |  | 7 | 2.92 |
| 15 |  | 7 | 2.92 |
| 16 |  | 7 | 2.92 |
| 17 |  | 7 | 2.92 |
| 18 |  | 7 | 2.92 |
| 19 |  | 7 | 2.92 |
| 20 |  | 6 | 2.50 |

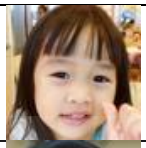
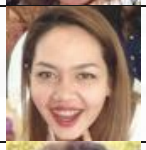
ตารางที่ 4.96 (ต่อ)

*ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่านแบบไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 21 |  | 6 | 2.50 |
| 22 |  | 6 | 2.50 |
| 23 |  | 6 | 2.50 |
| 24 |  | 6 | 2.50 |
| 25 |  | 6 | 2.50 |
| 26 |  | 6 | 2.50 |
| 27 |  | 5 | 2.08 |
| 28 |  | 5 | 2.08 |
| 29 |  | 5 | 2.08 |
| 30 |  | 5 | 2.08 |

ตารางที่ 4.96 (ต่อ)

*ความถี่ของรูปภาพที่ถูกเลือกใช้เป็นรหัสผ่านแบบไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท*

| ลำดับ | รูปภาพ | จำนวนความถี่ที่ถูกเลือกใช้ | ร้อยละ |
|---|---|---|---|
| 31 |  | 4 | 1.67 |
| 32 |  | 4 | 1.67 |
| 33 |  | 3 | 1.25 |
| 34 |  | 3 | 1.25 |
| 35 |  | 2 | .83 |
| 36 |  | 1 | .42 |

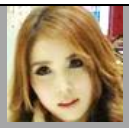
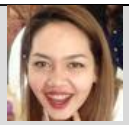
### 4.5.3 ผลการวิเคราะห์ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้

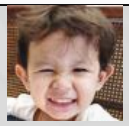
การวิเคราะห์ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ โดยการวิเคราะห์ตำแหน่งของรูปภาพที่ถูกเลือกเพื่อตั้งเป็นรหัสผ่าน จากตำแหน่งของรูปภาพทั้ง 36 ช่อง โดยแยกตามปัจจัยจำนวนรอบในการตั้งรหัสผ่าน และปัจจัยการมีกฎในการเลือกรหัสผ่าน จากการทดลองสามารถสรุปผลการวิเคราะห์ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ ได้ดังนี้

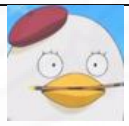
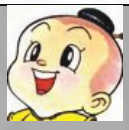
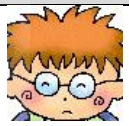
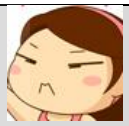
ตารางที่ 4.95

*ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มทดลองที่ 1 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ*

| | | |
|---|---|---|
|  1.67 |  6.67 |  1.67 |
|  0.83 |  5.00 |  1.67 |
|  2.50 |  1.67 |  3.33 |

| | | |
|---|---|---|
|  1.67 |  7.50 |  3.33 |
|  2.50 |  1.67 |  0.83 |
|  2.50 |  1.67 |  3.33 |

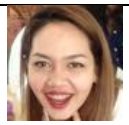
| | | |
|---|---|---|
|  0.83 |  2.50 |  5.00 |
|  0.83 |  3.33 |  0.00 |
|  1.67 |  1.67 |  9.17 |

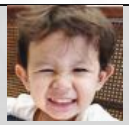
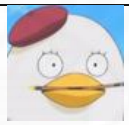
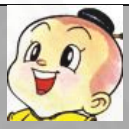
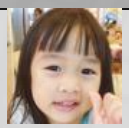
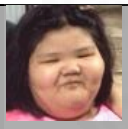
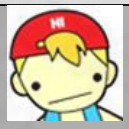
| | | |
|---|---|---|
|  1.67 |  6.67 |  4.17 |
|  4.17 |  0.00 |  0.00 |
|  2.50 |  1.67 |  4.17 |

จากตารางที่ 4.95 ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มทดลองที่ 1 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ พบว่า การเลือกรูปภาพเพื่อตั้งเป็นรหัสผ่านไม่ได้เลือกจากตำแหน่งของรูปภาพ เนื่องจากจะเห็นได้ว่าความถี่ของตำแหน่งรูปภาพที่ถูกเลือกมีการกระจัดกระจาย ไม่ขึ้นอยู่กับตำแหน่งใดตำแหน่งหนึ่ง

ตารางที่ 4.96

*ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มทดลองที่ 2 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท*

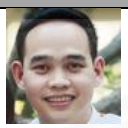
| | | | | | |
|---|---|---|---|---|---|
|  |  |  |  |  |  |
| 3.33 | 1.67 | 0.83 | 0.83 | 2.50 | 0.83 |
|  |  |  |  |  |  |
| 1.67 | 4.17 | 2.50 | 2.50 | 1.67 | 2.50 |
|  |  |  |  |  |  |
| 5.00 | 1.67 | 5.00 | 6.67 | 4.17 | 0.00 |

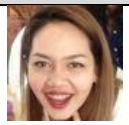
| | | | | | |
|---|---|---|---|---|---|
|  |  |  |  |  |  |
| 1.67 | 4.17 | 2.50 | 2.50 | 5.00 | 1.67 |
|  |  |  |  |  |  |
| 1.67 | 2.50 | 1.67 | 3.33 | 2.50 | 3.33 |
|  |  |  |  |  |  |
| 4.17 | 4.17 | 2.50 | 5.00 | 2.50 | 1.67 |

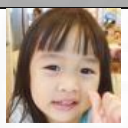
จากตารางที่ 4.96 ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มทดลองที่ 2 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท พบว่า การเลือกรูปภาพเพื่อตั้งเป็นรหัสผ่านไม่ได้เลือกจากตำแหน่งของรูปภาพ เนื่องจากจะเห็นได้ว่าความถี่ของตำแหน่งรูปภาพที่ถูกเลือกมีการกระจัดกระจาย ไม่ขึ้นอยู่กับตำแหน่งใดตำแหน่งหนึ่ง

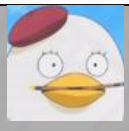
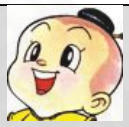
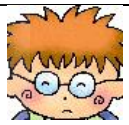
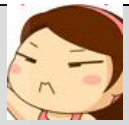
ตารางที่ 4.97

*ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มทดลองที่ 3 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ*

| | | |
|---|---|---|
|  3.33 |  2.50 |  0.83 |
|  4.17 |  5.00 |  2.50 |
|  3.33 |  1.67 |  1.67 |

| | | |
|---|---|---|
|  3.33 |  3.33 |  0.83 |
|  2.50 |  1.67 |  4.17 |
|  5.00 |  2.50 |  1.67 |

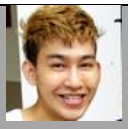
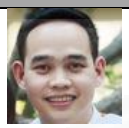
| | | |
|---|---|---|
|  4.17 |  5.83 |  2.50 |
|  1.67 |  1.67 |  0.00 |
|  1.67 |  5.00 |  2.50 |

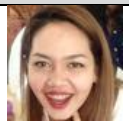
| | | |
|---|---|---|
|  5.00 |  4.17 |  2.50 |
|  2.50 |  0.83 |  1.67 |
|  1.67 |  2.50 |  4.17 |

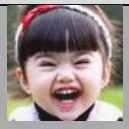
จากตารางที่ 4.97 ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มทดลองที่ 3 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับมีกฎในการเลือกรหัสผ่านรูปภาพประเภทละ 2 รูปภาพ พบว่า การเลือกรูปภาพเพื่อตั้งเป็นรหัสผ่านไม่ได้เลือกจากตำแหน่งของรูปภาพ เนื่องจากจะเห็นได้ว่าความถี่ของตำแหน่งรูปภาพที่ถูกเลือกมีการกระจัดกระจาย ไม่ขึ้นอยู่กับตำแหน่งใดตำแหน่งหนึ่ง

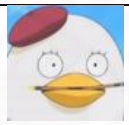
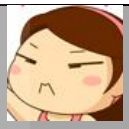
ตารางที่ 4.98

*ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มทดลองที่ 4 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท*

| | | |
|---|---|---|
|  2.50 |  4.17 |  0.00 |
|  4.17 |  4.17 |  3.33 |
|  2.50 |  1.67 |  3.33 |

| | | |
|---|---|---|
|  0.83 |  2.50 |  3.33 |
|  5.00 |  0.83 |  4.17 |
|  3.33 |  1.67 |  2.50 |

| | | |
|---|---|---|
|  2.50 |  3.33 |  2.50 |
|  3.33 |  0.83 |  3.33 |
|  3.33 |  3.33 |  5.83 |

| | | |
|---|---|---|
|  2.50 |  2.50 |  3.33 |
|  3.33 |  1.67 |  1.67 |
|  0.83 |  1.67 |  4.17 |

จากตารางที่ 4.98 ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ของกลุ่มทดลองที่ 4 ใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านรูปภาพในแต่ละประเภท พบว่า การเลือกรูปภาพเพื่อตั้งเป็นรหัสผ่านไม่ได้เลือกจากตำแหน่งของรูปภาพ เนื่องจากจะเห็นได้ว่าความถี่ของตำแหน่งรูปภาพที่ถูกเลือกมีการกระจัดกระจาย ไม่ขึ้นอยู่กับตำแหน่งใดตำแหน่งหนึ่ง

# บทที่ 5
# สรุปผลการวิจัยและข้อเสนอแนะ

งานวิจัยนี้ทำการศึกษาเปรียบเทียบปัจจัยที่มีอิทธิพลต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยมีปัจจัยที่นำมาศึกษาเปรียบเทียบ 2 ปัจจัย ได้แก่ ปัจจัยจำนวนรอบในการตั้งรหัสผ่าน ระหว่างการใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ กับการใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ และปัจจัยการมีกฎในการเลือกรหัสผ่าน ระหว่างการมีกฎในการเลือกรหัสผ่านประเภทละ 2 รูปภาพ กับการไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท เพื่อวิเคราะห์ถึงปัจจัยที่มีอิทธิพลต่อด้านการใช้งาน ด้านความปลอดภัย และความพึงพอใจของผู้ใช้งาน โดยการวิเคราะห์ด้านการใช้งาน ใช้ข้อมูลจำนวนครั้งที่ใช้ในการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตน และความสำเร็จในการพิสูจน์ตัวตน สำหรับการวิเคราะห์ด้านความปลอดภัย ใช้ข้อมูลการโจรกรรมการพิสูจน์ตัวตนด้วยวิธีการแอบมอง (Shoulder surfing) โดยวิเคราะห์จาก จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน โดยข้อมูลที่นำมาวิเคราะห์ในด้านการใช้งานและด้านความปลอดภัย มาจากการทดลองทั้งหมด 3 ครั้ง ได้แก่ ครั้งที่ 1 ทดลองหลังจากการลงทะเบียนทันที ครั้งที่ 2 ทดลองหลังจากการลงทะเบียนไปแล้ว 3 วัน และครั้งที่ 3 ทดลองหลังจากการลงทะเบียนไปแล้ว 15 วัน และในส่วนของความพึงพอใจของผู้ใช้วิเคราะห์จากคะแนนของแบบสอบถามความพึงพอใจที่มีต่อโปรแกรมการพิสูจน์ตัวตนที่ออกแบบ โดยในบทนี้จะนำเสนอการสรุปผลการวิจัยด้านการใช้งาน ด้านความปลอดภัย และด้านความพึงพอใจ พร้อมทั้งการอภิปรายผล ข้อเสนอแนะ และแนวทางการวิจัยในอนาคต ดังนี้

## 5.1 สรุปผลการวิจัย

ผลการวิจัยของงานวิจัยนี้ จะประกอบไปด้วย ผลการทดลองด้านการใช้งาน ผลการทดลองด้านความปลอดภัย และคะแนนความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อโปรแกรมพิสูจน์ตัวตน มีรายละเอียดดังนี้

### 5.1.1 ด้านการใช้งาน (Usability)

ผลการวิเคราะห์การทดลองด้านการใช้งานทั้ง 3 ครั้ง ประกอบไปด้วย ครั้งที่ 1 หลังจากสร้างรหัสผ่านทันที ครั้งที่ 2 หลังจากสร้างรหัสผ่าน 3 วัน ครั้งที่ 3 หลังจากสร้างรหัสผ่าน 15 วัน พบว่า ในการทดลองครั้งที่ 2 ปัจจัยจำนวนรอบในการตั้งรหัสผ่านมีอิทธิพลต่อการใช้งานอย่างมีนัยสำคัญทางสถิติต่อ จำนวนครั้งในการพิสูจน์ตัวตนและความสำเร็จในการพิสูจน์ตัวตน ซึ่งสอดคล้อง

กับสมมติฐานที่ตั้งไว้คือ จำนวนรอบในการตั้งรหัสผ่าน มีอิทธิพลต่อการใช้งานรหัสผ่านรูปภาพ โดยเมื่อวิเคราะห์การมีอิทธิพลร่วมของทั้ง 2 ปัจจัย กลุ่มทดลองที่ใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยที่สุด มีเวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตนน้อยที่สุด และมีคะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด

### 5.1.2 ด้านความปลอดภัย (Security)

ผลการวิเคราะห์ผลการทดลองด้านความปลอดภัย ประกอบไปด้วย จำนวนครั้งที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน เวลาเฉลี่ยที่ใช้ในการโจรกรรมการพิสูจน์ตัวตน และความสำเร็จในการโจรกรรมการพิสูจน์ตัวตน ของการทดลองทั้ง 3 ครั้ง ได้แก่ ครั้งที่ 1 ทดลองการโจรกรรมการพิสูจน์ตัวตนหลังจากลงทะเบียนทันที ครั้งที่ 2 ทดลองการโจรกรรมการพิสูจน์ตัวตนหลังจากลงทะเบียน 3 วัน ครั้งที่ 3 ทดลองการโจรกรรมการพิสูจน์ตัวตนหลังจากลงทะเบียน 15 วัน นั้น พบว่า ผลการทดลองด้านความปลอดภัย ไม่มีผู้เข้าร่วมการทดลองที่ทำการโจรกรรมการพิสูจน์ตัวตนได้ได้สำเร็จ ซึ่งแสดงว่า การทดลองทั้ง 4 กลุ่มทดลองมีความปลอดภัยจากการโจรกรรมการพิสูจน์ตัวตนด้วยวิธีการแอบมอง (Shoulder surfing) 100 เปอร์เซ็นต์ แสดงให้เห็นว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านและปัจจัยการมีกฎในการเลือกรหัสผ่าน ไม่มีอิทธิพลต่อความปลอดภัยของรหัสผ่านรูปภาพ

### 5.1.3 ด้านความพึงพอใจ

ผลการวิเคราะห์ความพึงพอใจของผู้เข้าร่วมการทดลองที่มีต่อโปรแกรมการพิสูจน์ตัวตน พบว่า ปัจจัยจำนวนรอบในการตั้งรหัสผ่านไม่มีอิทธิพลต่อความความพึงพอ ปัจจัยการมีกฎในการเลือกรหัสผ่านไม่มีอิทธิพลต่อความความพึง และทั้งสองปัจจัยไม่มีอิทธิพลร่วมต่อความความพึงพอ โดยมีคะแนนความความพึงพอใจต่อระบบการพิสูจน์ตัวตนที่ได้ออกแบบโดยรวมอยู่ในระดับพึงพอใจมาก

## 5.2 ประโยชน์ของงานวิจัย

### 5.2.1 ประโยชน์ของงานวิจัยเชิงทฤษฎี (Theoretical Implications)

จากงานวิจัยได้ค้นพบว่า ระบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพในลักษณะของงานวิจัยนี้ใช้งานง่ายและมีความปลอดภัยสูง ควรที่จะใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 1 รอบ เพราะส่งผลต่อด้านการใช้งานที่ดีกว่าการใช้จำนวนรอบในการตั้งรหัสผ่านรูปภาพ 2 รอบ และไม่จำเป็นต้องมีกฎในการเลือกรหัสผ่านรูปภาพ เพราะการมีกฎในการเลือกรหัสผ่านรูปภาพหรือการไม่มีกฎในการเลือกรหัสผ่านรูปภาพ ไม่ได้ส่งผลต่อด้านการใช้งานและด้านความปลอดภัยด้วยวิธีการ

แอบมอง (Shoulder surfing) และค้นพบว่ารูปภาพใบหน้าที่นำมาใช้ในระบบอาจไม่จำเป็นต้องเป็นใบหน้าบุคคลที่เป็นที่รู้จักหรือมีชื่อเสียง ถ้าระบบมีการออกแบบที่ดี เพราะจะเห็นได้ว่าระบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพของงานวิจัยนี้ ใช้รูปภาพใบหน้าที่ไม่เป็นที่รู้จักหรือมีชื่อเสียง ผู้ใช้งานก็สามารถใช้งานได้และมีความพึงพอใจในระดับมาก

### 5.2.2 ประโยชน์ของงานวิจัยเชิงประยุกต์ (Practical Implications)

การนำไปประยุกต์ใช้เพื่อพัฒนาซอฟต์แวร์ ควรเลือกใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ เนื่องจากการใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ ส่งผลต่อการใช้งานที่ง่ายกว่าการเลือกใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ และในด้านความปลอดภัยนั้นไม่แตกต่างกัน ในส่วนของปัจจัยการมีกฎในการเลือกรหัสผ่าน ควรเลือกใช้การไม่มีกฎในการเลือกรหัสผ่าน เนื่องจากจะทำให้การพัฒนาซอฟต์แวร์ทำได้ง่าย ไม่ต้องกำหนดเงื่อนไขตามกฎที่ซับซ้อน และในด้านความปลอดภัยถึงแม้ว่าไม่ส่งผลต่อความปลอดภัยด้วยวิธีการแอบมอง (Shoulder surfing) แต่ในแง่ของการคาดเดารหัสผ่านจะมีความปลอดภัยมากกว่าการมีกฎในการเลือกรหัสผ่าน เนื่องจากการไม่มีกฎในการเลือกรหัสผ่านมีความเป็นไปได้ของรหัสผ่านมากกว่าการมีกฎในการเลือกรหัสผ่าน

## 5.3 การอภิปรายผลและข้อเสนอแนะ

งานวิจัยนี้ทำการศึกษาเปรียบเทียบปัจจัยที่มีอิทธิพลต่อวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยปัจจัยที่นำมาศึกษาเปรียบเทียบ ได้แก่ จำนวนรอบในการตั้งรหัสผ่านกับการมีกฎในการลือกรหัสผ่าน เพื่อหารูปแบบวิธีการพิสูจน์ตัวตนที่มีการใช้งานที่ง่าย (Usability) และมีความปลอดภัย (Security) โดยนำเอารูปแบบการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่มีลักษณะเดียวกับ S-Passface มาประยุกต์ใช้ในการออกแบบ เนื่องจากมีความปลอดภัยจากการโจรกรรมการพิสูจน์ตัวตน ด้วยวิธีการแอบมอง (Shoulder surfing) ถึง 100 เปอร์เซ็นต์ แต่ในด้านการใช้งานพบว่าความง่ายในการใช้งานลดลงเมื่อเทียบกับวิธี Passface ผู้วิจัยเห็นว่าเพื่อประโยชน์ของผู้ใช้งานในการเก็บรักษาข้อมูลที่สำคัญในระบบเทคโนโลยีสารสนเทศ และเพื่อวิเคราะห์หารูปแบบในการออกแบบและพัฒนา วิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพที่สามารถใช้งานง่าย (Usability) และมีความปลอดภัย (Security) ผู้วิจัยจึงสนใจนำเอารูปแบบวิธีการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพแบบ S-Passface มาประยุกต์ใช้เพื่อการศึกษาถึงปัจจัยที่มีอิทธิพลต่อการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ โดยมีปัจจัยที่นำมาศึกษาเปรียบเทียบ 2 ปัจจัย ได้แก่ จำนวนรอบในการตั้งรหัสผ่าน ระหว่างการใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ และการใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ และปัจจัยการมีกฎในการเลือกรหัสผ่าน ระหว่างการมีกฎในการเลือกรหัสผ่านประเภทละ 2 รูปภาพ และการไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท มาใช้ในการออกแบบระบบการพิสูจน์ตัวตน เพื่อวิเคราะห์ถึงปัจจัยที่มีอิทธิพลต่อด้านการใช้งาน ด้านความปลอดภัย และความพึงพอใจของผู้ใช้งาน ซึ่งพบว่า

การใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ ร่วมกับไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท ใช้จำนวนครั้งในการพิสูจน์ตัวตนน้อยที่สุด มีเวลาเฉลี่ยที่ใช้ในการพิสูจน์ตัวตนน้อยที่สุด คะแนนความสำเร็จในการพิสูจน์ตัวตนมากที่สุด และในการวิเคราะห์ความเป็นไปได้ทั้งหมดของรหัสผ่าน (Password space) พบว่า มีความเป็นไปได้ของรหัสผ่านมากที่สุด การวิเคราะห์ความถี่ของตำแหน่งรูปภาพที่ถูกเลือกใช้ พบว่า การเลือกรูปภาพเพื่อตั้งเป็นรหัสผ่านไม่ได้เลือกจากตำแหน่งของรูปภาพเนื่องจากความถี่ของตำแหน่งรูปภาพที่ถูกเลือกมีการกระจัดกระจาย ไม่ขึ้นอยู่กับตำแหน่งใดตำแหน่งหนึ่ง

ในด้านข้อเสนะแนะของรูปภาพที่เป็นตัวเลือกในการตั้งรหัสผ่าน เป็นสิ่งสำคัญต่อการสร้างรหัสผ่านรูปภาพ เนื่องจากผู้เข้าร่วมการทดลองจะพยายามหาเอกลักษณ์ และความสัมพันธ์ของรูปภาพตัวเลือก เพื่อการเชื่อมโยงให้สามารถจดจำได้ง่าย ดังนั้นจึงควรเลือกรูปภาพที่จะนำมาใช้เป็นตัวเลือกที่มีความคมชัดและมีเอกลักษณ์ที่ชัดเจน

## 5.4 แนวทางการวิจัยในอนาคต

เพื่อให้งานวิจัยการพิสูจน์ตัวตนด้วยรหัสภาพรูปภาพในลักษณะนี้ มีประสิทธิภาพด้านการใช้งานและประสิทธิภาพด้านความปลอดภัยดีขึ้นนั้น สิ่งที่สำคัญประการหนึ่ง คือการเลือกรูปภาพเพื่อนำมาเป็นตัวเลือกรหัสผ่านรูปภาพ โดยธรรมชาติของผู้ใช้จะเลือกรูปภาพที่มีความโดดเด่น เช่น รูปภาพใบหน้าที่ใส่แว่นตา หรือใบหน้าที่มีการแสดงอารมณ์อย่างโดดเด่น ทำให้ผู้ใช้มีแนวโน้มเลือกรูปภาพที่โดดเด่น จะทำให้ความปลอดภัยลดลงและอาจจะถูกโจรกรรมได้ง่าย ดังนั้นควรให้ความสำคัญในการเลือกรูปภาพเพื่อนำมาเป็นตัวเลือกรหัสผ่านรูปภาพที่มีความโดดเด่น และในด้านการพัฒนาวิธีดำเนินงานวิจัย โดยทำการทดลองกับกลุ่มตัวอย่างที่มีจำนวนมากขึ้น เพื่อให้ผลที่ได้จากการทดลองมีความหลากหลายและครอบคลุมพฤติกรรมหรือแนวคิดของแต่ละบุคคลซึ่งอาจมีความแตกต่างกัน เช่น การใช้เทคนิคในการสร้างรหัสผ่าน หรือการเรียบเรียงรหัสผ่านให้ง่ายต่อการจดจำ เป็นต้น เพื่อให้ผลการทดลองมีความน่าเชื่อถือมากยิ่งขึ้น และเพิ่มจำนวนครั้งและระยะเวลาในการทำการทดลองการพิสูจน์ตัวตนให้ยาวนานขึ้น เพื่อสามารถวิเคราะห์ประสิทธิภาพด้านการใช้งานในระยะยาว

# รายการอ้างอิง


**หนังสือ**

กัลยา วานิชย์บัญชา. (2548). *การใช้ SPSS for windows ในการวิเคราะห์ข้อมูล.* (พิมพ์ครั้งที่ 7). กรุงเทพฯ: ภาควิชาสถิติ คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย.

ธานินทร์ ศิลป์จารุ. (2552). *การวิจัยและวิเคราะห์ข้อมูลทางสถิติด้วย SPSS.* (พิมพ์ครั้งที่ 10). กรุงเทพฯ: บิสซิเนสอาร์แอนด์ดี.

อุบลรัตน์ เพ็งสถิต. (2535). *ความจำมนุษย์.* (พิมพ์ครั้งที่ 5). กรุงเทพฯ: มหาวิทยาลัยรามคำแหง.

**บทความวารสาร**

อำนาจ วังจีน. (2550). ทางออกของการใช้ One-Way ANOVA กับการวิจัยทางสังคมศาสตร์เมื่อข้อมูลไม่เป็นไปตามข้อกำหนด. *วารสารศรีปทุมปริทัศน์ ปีที่ 7 ฉบับที่ 1 มกราคม-มิถุนายน*

**วิทยานิพนธ์**

คณิน อุดมสุขประเสริฐ. (2555). *การศึกษาพฤติกรรมการตั้งรหัสผ่านของผู้ใช้งานอินเทอร์เน็ตวัยทำงานในประเทศไทย*. (วิทยานิพนธ์ปริญญามหาบัณฑิต). มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ, คณะเทคโนโลยีสารสนเทศ.

ดนุพัฒน์ กชชาดาปภาดา. (2556). *ปัจจัยที่ส่งผลต่อรหัสผ่านรูปภาพแบบกริด : วิธีการสร้างรหัสผ่านและประเภทของภาพ*. (วิทยานิพนธ์ปริญญามหาบัณฑิต). มหาวิทยาลัยธรรมศาสตร์, คณะวิทยาศาสตร์และเทคโนโลยี.

**Articles**

Akpulat, M., Bicakci, K., & Cil, U. (2013). Revisiting Graphical Passwords for Augmenting, not Replacing, Text Passwords. *ACSAC 2013 : 29th Annual Computer Security Applications Conference,* 119-128.

Chaudhari, S. K., Deshpande, A. R., Bendale, S. B., & Kotian, R. V. (2011), 3D Drag-n-Drop CAPTCHA Enhanced Security through CAPTCHA. *International Conference and Workshop on Emerging Trends in Technology (ICWET 2011)*, 598-601.

Forget, A., Chiasson, S., Oorschot, V., & Biddle, R. (2008). Improving Text Passwords Through Persuasion. *Symposium on Usable Privacy and Security (SOUPS).*

Kotadia, M. (2005). Microsoft: Write down your passwords. ZDNet Australia. May 23.

Lashkari, A. H., Zakaria, O. B., Farmand, S., & Saleh, R. (2009). Shoulder Surfing attack in graphical password authentication. *(IJCSIS) International Journal of Computer Science and Information Security Vol. 6, No. 2*, 145-154.

Morris, R., & Thompson, K. (1979). Password security: A case history. *Communications of the ACM (11),* 594-597.

Qureshi, M., Younus, A., & Khan, A. A. (2009). Philosophical Survey of Passwords. *IJCSI International Journal of Computer Science Issues Vol. 2*, 8-12.

Tari, F., Ozok, A. A., & Holden, S. H. (2006). A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical Passwords. *Symposium On Usable Privacy and Security (SOUPS),* 56-66.

Farnaz, T., Maslin, M., & Azizah, A. M. (2013). An Enhancement on Passface Graphical Password Authentication. *Journal of Basic and Applied Scientific Research*. Vol. 3(2), 135-141

Wu, T. (1990). A real-world analysis of Kerebros password security. *In Proceedings of the 1999ISOC Symposium on Network and Distributed System Security 9,* Vol. 8, 723-736.

**Conference**

Dhamija, R., & Perrig, A. (2000). Déjà vu: A User Study Using Images for Authentication. *In Proceedings of 9th USENIX Security Symposium*.

Feldmeier, D., & Karn, P. (1989). UNIX password security-Ten years later. *In Proceedings of the 19th International Conference on Advances in Cryptology (CRYPTO '89).* Lecture Notes in Computer Science, Vol. 435.

Paivio, A., Rogers, T. B., & Smythe, P. C. (1968). Why are pictures easier to recall than words*?. Psychonomic Science*, pp. 11:137-138.

# ภาคผนวก

# ภาคผนวก ก
# แบบสอบถาม

## ส่วนที่ 1 แบบสอบถามข้อมูลทั่วไป

คำชี้แจง โปรดทำเครื่องหมาย ✓ ลงในช่อง ☐ ที่ตรงกับข้อมูลของท่าน

1. เพศ :

☐ ชาย ☐ หญิง

2. อายุ :

☐ ต่ำกว่า 20 ปี ☐ 21-30 ปี ☐ 31-40 ปี ☐ 41-50 ปี ☐ 51 ปีขึ้นไป

3. ระดับการศึกษา :

☐ ต่ำกว่าปริญญาตรี ☐ ปริญญาตรี ☐ สูงกว่าปริญญาตรี

4. ความถี่ในการใช้คอมพิวเตอร์ :

☐สัปดาห์ละ 1-3 วัน ☐ สัปดาห์ละ 4-6 วัน ☐ สัปดาห์ละ 7 วัน

5. ท่านเคยใช้วิธีการพิสูจน์ตัวตนแบบใดบ้าง :

☐ ระบบพิสูจน์ตัวตนที่ใช้ตัวอักษรเป็นรหัสผ่าน

☐ ระบบพิสูจน์ตัวตนที่ต้องใช้งานควบคู่กับอุปกรณ์จำพวกการ์ด เช่น การใช้บัตร ATM, การใช้บัตรเข้า-ออกประตู เป็นต้น

☐ ระบบพิสูจน์ตัวตนแบบใช้เอกลักษณ์เฉพาะตัวบุคคล เช่น การสแกนลายนิ้วมือ การใช้ใบหน้าในการพิสูจน์ตัวตน เป็นต้น

☐ ระบบพิสูจน์ตัวตนด้วยการใช้รูปภาพเป็นรหัสผ่าน

☐ อื่นๆ โปรดระบุ.....

6. กรณีที่คุณมีหลายบัญชี เช่น Hotmail, Gmail, Facebook, Internet banking เป็นต้น คุณมักจะ :

☐ ตั้งรหัสผ่านเหมือนกันทุกบัญชี

☐ ตั้งรหัสผ่านแตกต่างกันทุกบัญชี

☐ ตั้งรหัสผ่านเหมือนกันบางบัญชี

7. โดยทั่วไปแล้วท่านมีวิธีเก็บรักษารหัสผ่านอย่างไร :

☐ ใช้วิธีการจดบันทึก ☐ ใช้วิธีการจำ ☐ อื่นๆ โปรดระบุ.....

8. ท่านเคยลืมรหัสผ่าน (Password) บ่อยขนาดไหน :

| | 0 | 1 | 2 | 3 | 4 | |
|---|---|---|---|---|---|---|
| ไม่เคย | ☐ | ☐ | ☐ | ☐ | ☐ | บ่อยที่สุด |

**ส่วนที่ 2 แบบสอบถามความพึงพอใจ**

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงกับความพึงพอใจของท่าน

ระดับคะแนนความพึงพอใจ มี 5 ระดับ คือ

5 หมายถึงระดับความพึงพอใจมากที่สุด

4 หมายถึงระดับความพึงพอใจมาก

3 หมายถึงระดับความพึงพอใจปานกลาง

2 หมายถึงระดับความพึงพอใจน้อย

1 หมายถึงระดับความพึงพอใจน้อยที่สุด

ตารางที่ ก. 1

*รายละเอียดแบบสอบถามความพึงพอใจ*

| ข้อที่ | รายละเอียด | ระดับคะแนนความพึงพอใจ | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 1 | การสร้างรหัสผ่านในขั้นตอนการลงทะเบียนทำได้ง่าย | | | | | |
| 2 | วิธีการใส่รหัสผ่านทำได้ง่าย | | | | | |
| 3 | รหัสผ่านรูปภาพจดจำได้ง่าย | | | | | |
| 4 | ขั้นตอนในการลงทะเบียนและการเข้าสู่ระบบง่าย ไม่ซับซ้อน | | | | | |
| 5 | ขั้นตอนการทำงานรวดเร็ว | | | | | |
| 6 | ความพึงพอใจต่อรูปภาพ มีความชัดเจน มีเอกลักษณ์ | | | | | |
| 7 | ความพึงพอใจต่อส่วนต่อประสาน หน้าจอการใช้งาน เหมาะสม | | | | | |
| 8 | โปรแกรมสามารถเข้าใจได้ง่าย | | | | | |
| 9 | โปรแกรมนี้มีความน่าเชื่อถือสามารถนำไปใช้งานได้จริง | | | | | |

| ข้อที่ | รายละเอียด | ระดับคะแนนความพึงพอใจ | | | | |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 10 | ในด้านความปลอดภัย คุณคิดว่าวิธีการนี้มีความความปลอดภัย | | | | | |
| 11 | ในด้านการใช้งาน คุณคิดว่าวิธีการนี้ใช้งานง่าย | | | | | |

**ส่วนที่ 3 ข้อคิดเห็นเพิ่มเติมเกี่ยวกับโปรแกรมการพิสูจน์ตัวตนที่ออกแบบ**

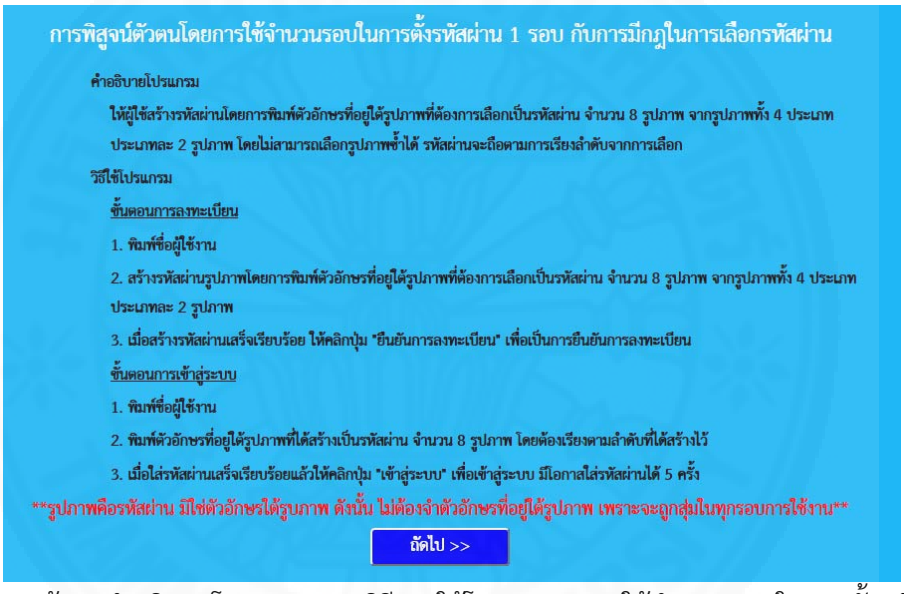
.....

.....

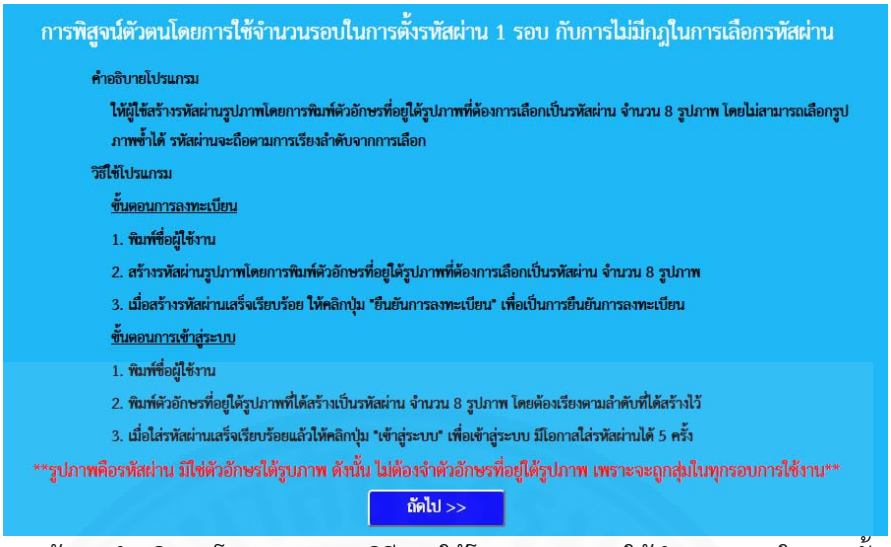
# ภาคผนวก ข
# โปรแกรมที่ใช้ในการทดลอง

## ข. 1 หน้าจอคำอธิบายโปรแกรมและวิธีการใช้โปรแกรม

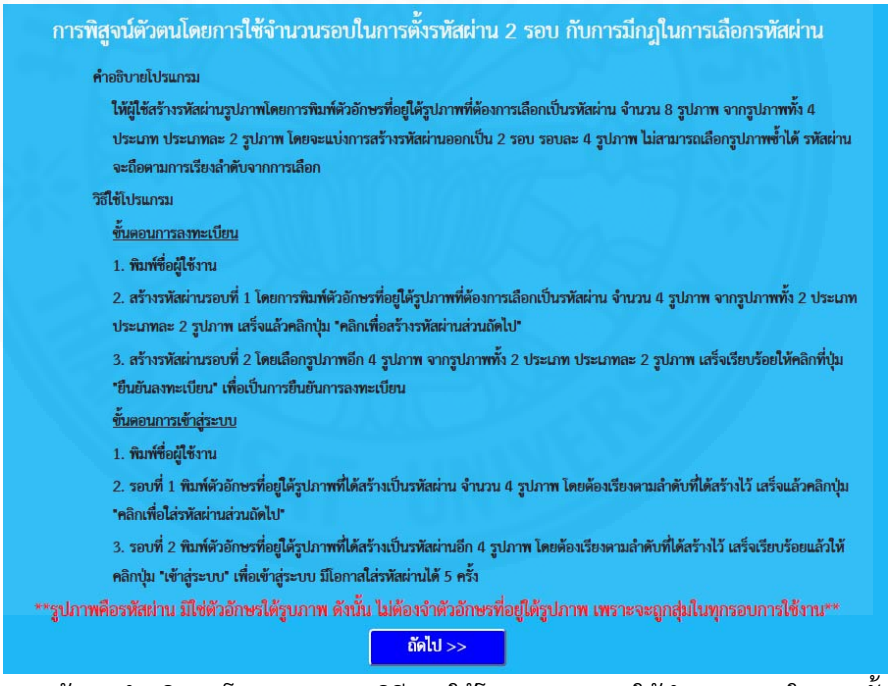
เมื่อเปิดโปรแกรมจะพบกับหน้าจอคำอธิบายโปรแกรมและวิธีการใช้โปรแกรม ซึ่งคำอธิบายจะแตกต่างกันตามโปรแกรมของกลุ่มทดลองนั้น ๆ โดยเมื่อผู้เข้าร่วมการทดลองเข้าใจวิธีการใช้งานแล้วให้คลิกปุ่ม "ถัดไป" เพื่อไปหน้าจอทดลองใช้งาน



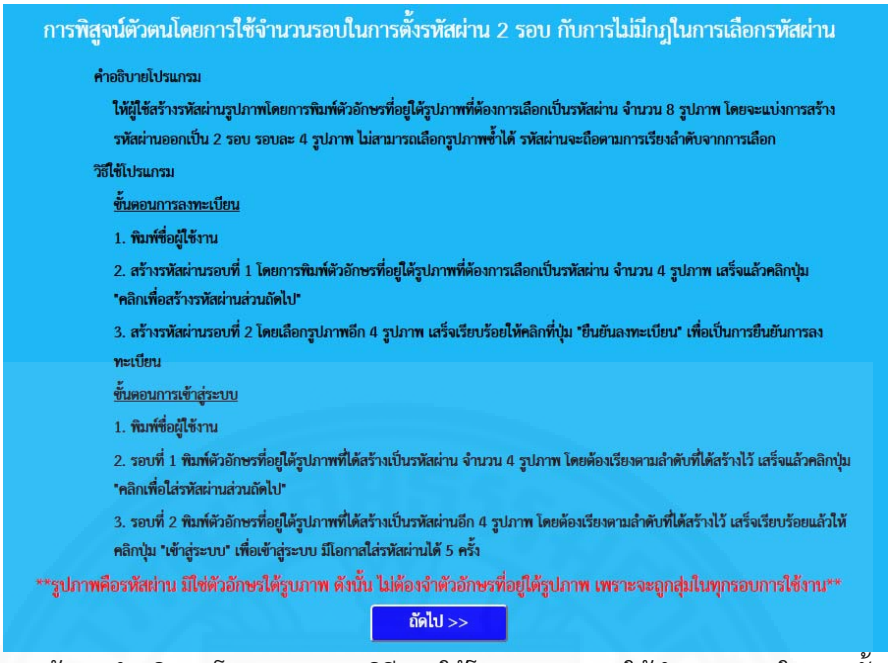

*ภาพที่ ข.1* หน้าจอคำอธิบายโปรแกรมและวิธีการใช้โปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบกับการมีกฎในการเลือกรหัสผ่านประเภทละ 2 รูปภาพ




*ภาพที่ ข.2* หน้าจอคำอธิบายโปรแกรมและวิธีการใช้โปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบกับการไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท




*ภาพที่ ข. 3* หน้าจอคำอธิบายโปรแกรมและวิธีการใช้โปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบกับการมีกฎในการเลือกรหัสผ่านประเภทละ 2 รูปภาพ




*ภาพที่ ข. 4* หน้าจอคำอธิบายโปรแกรมและวิธีการใช้โปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบกับการไม่มีกฎในการเลือกรหัสผ่านในแต่ละประเภท

**ข. 2 หน้าจอทดลองใช้งาน**

หน้าจอทดลองใช้งาน เพื่อให้ผู้เข้าร่วมการทดลองได้ลองใช้งานให้เกิดความคุ้นเคยในการใช้งาน ซึ่งหน้าจอโปรแกรมจะมี 2 แบบ คือ แบบใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ และแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ เมื่อผู้เข้าร่วมการทดลองเกิดความคุ้นเคยในการใช้งานแล้วให้คลิกปุ่ม "เริ่มการทดลอง" เพื่อไปหน้าจอแบบสอบถามข้อมูลทั่วไป


*ภาพที่ ข.5* หน้าจอทดลองใช้งานของโปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ


*ภาพที่ ข.6* หน้าจอทดลองใช้งานของโปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ (รอบที่ 1)


*ภาพที่ ข.7* หน้าจอทดลองใช้งานของโปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ (รอบที่ 2)

**ข. 3 หน้าจอแบบสอบถามข้อมูลทั่วไป**

หน้าจอแบบสอบถามข้อมูลทั่วไป ให้ผู้เข้าร่วมการทดลองตอบแบบสอบถามข้อมูลทั่วไป แล้วคลิกปุ่ม "ถัดไป" เพื่อไปหน้าจอลงทะเบียน


*ภาพที่ ข.8* หน้าจอแบบสอบถามข้อมูลทั่วไป

**ข. 4 หน้าจอลงทะเบียน**

หน้าจอลงทะเบียน ให้ผู้เข้าร่วมการทดลองตั้งรหัสผ่านรูปภาพ แล้วคลิกปุ่ม "ยืนยันการลงทะเบียน" เพื่อทำการลงทะเบียน และโปรแกรมจะไปหน้าจอเข้าสู่ระบบ


*ภาพที่ ข.9* หน้าจอลงทะเบียนของโปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ


*ภาพที่ ข.10* หน้าจอลงทะเบียนของโปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ (รอบที่ 1)


*ภาพที่ ข.11* หน้าจอลงทะเบียนของโปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ (รอบที่ 2)

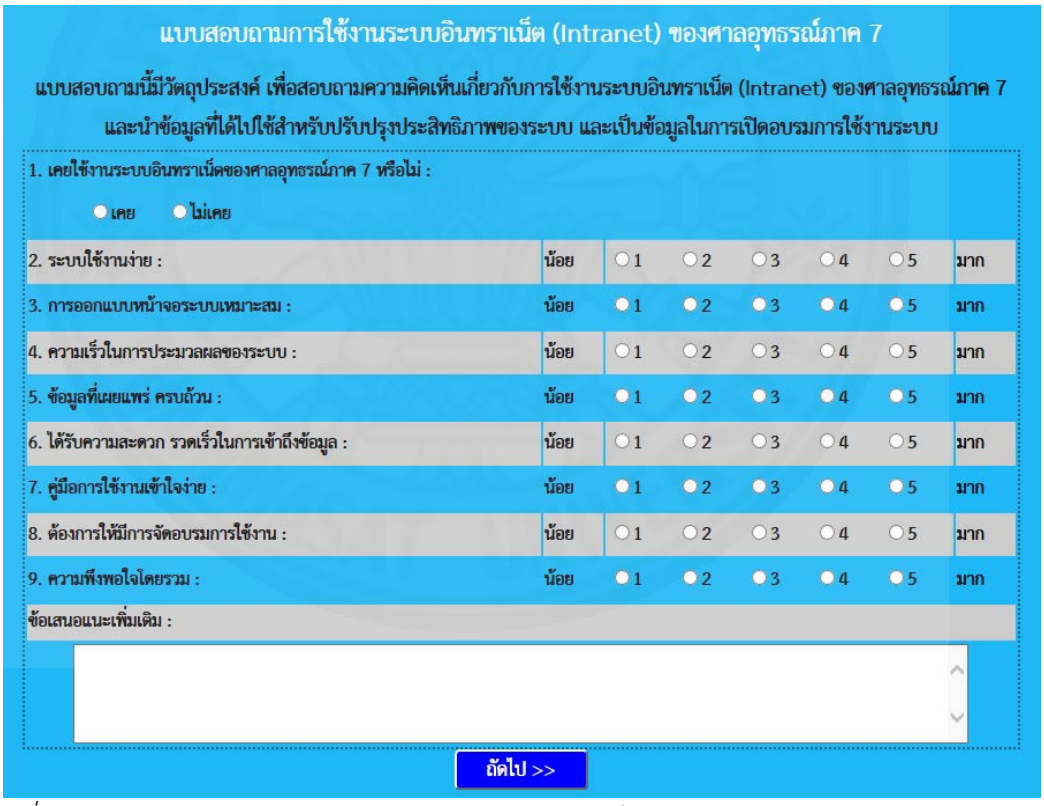
**ข. 5 หน้าจอเข้าสู่ระบบ**

หน้าจอเข้าสู่ระบบ ให้ผู้เข้าร่วมการทดลองทำการพิสูจน์ตัวตนโดยการใส่รหัสผ่านรูปภาพ แล้วคลิกปุ่ม "เข้าสู่ระบบ" โดยหากสามารถพิสูจน์ตัวตนสำเร็จ จะปรากฏหน้าจอแบบสอบถามที่ได้เอามาใช้ร่วมกับการทดลอง และเมื่อตอบแบบสอบถามเสร็จให้คลิกปุ่ม "ถัดไป" จะปรากฏหน้าจอขอขอบคุณที่ให้ความร่วมมือในการตอบแบบสอบถามครับ แต่หากทำการพิสูจน์ตัวตนไม่สำเร็จครบ 5 ครั้ง จะปรากฏหน้าจอเข้าสู่ระบบไม่สำเร็จ

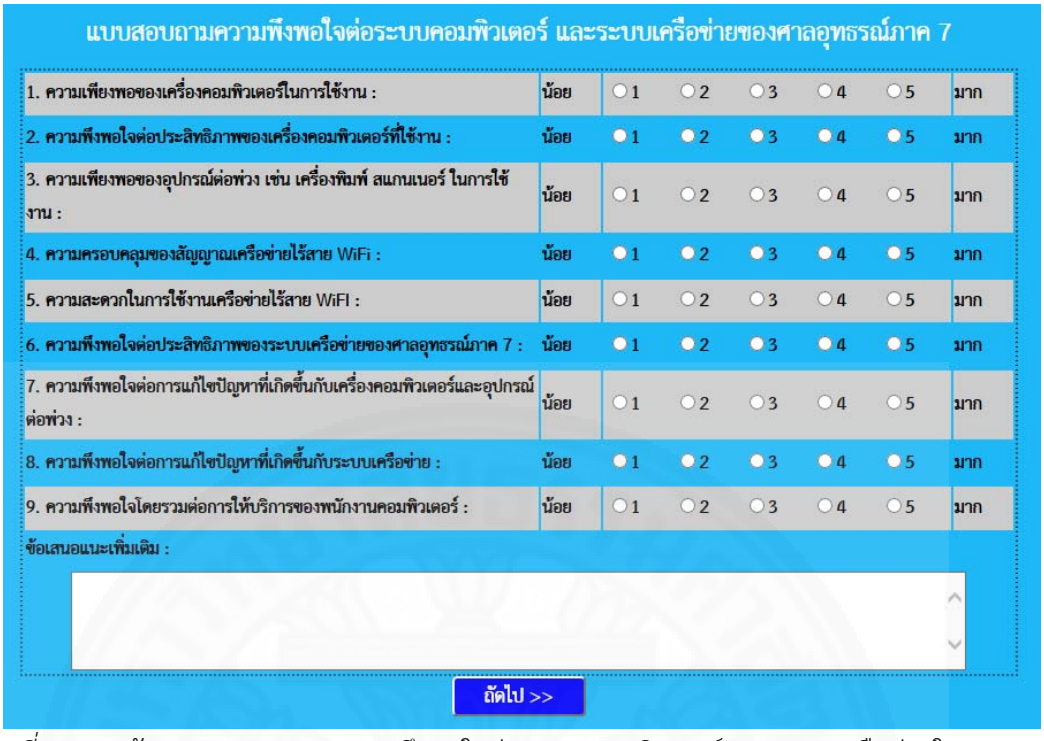

*ภาพที่ ข.12* หน้าจอเข้าสู่ระบบของโปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 1 รอบ


*ภาพที่ ข.13* หน้าจอเข้าสู่ระบบของโปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ (รอบที่ 1)

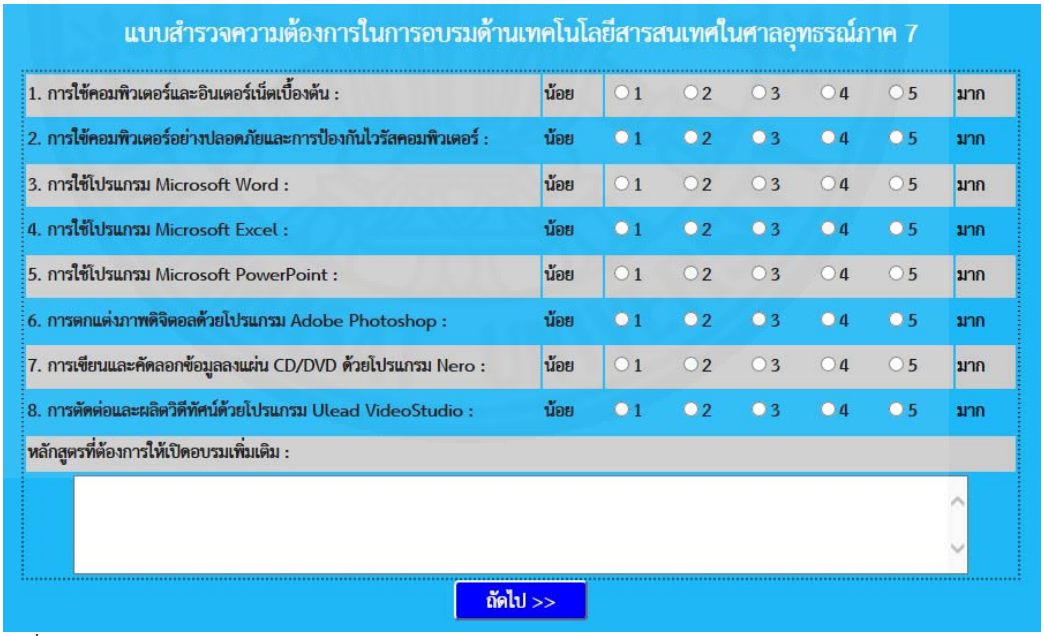

*ภาพที่ ข.14* หน้าจอเข้าสู่ระบบของโปรแกรมแบบใช้จำนวนรอบในการตั้งรหัสผ่าน 2 รอบ (รอบที่ 2)




*ภาพที่ ข.15* หน้าจอแบบสอบถามการใช้งานระบบอินทราเน็ต (Intranet) ของศาลอุทธรณ์ภาค 7




*ภาพที่ ข.16* หน้าจอแบบสอบถามความพึงพอใจต่อระบบคอมพิวเตอร์และระบบเครือข่ายในศาลอุทธรณ์ภาค 7




*ภาพที่ ข.17* หน้าจอแบบสำรวจความต้องการในการอบรมด้านเทคโนโลยีสารสนเทศในศาลอุทธรณ์ภาค 7


*ภาพที่ ข.18* หน้าจอขอขอบคุณที่ให้ความร่วมมือในการตอบแบบสอบถาม


*ภาพที่ ข.19* หน้าจอเข้าสู่ระบบไม่สำเร็จ

# ประวัติการศึกษา

| | |
|---|---|
| ชื่อ | นายธีรยุทธ เอกรุณ |
| วันเดือนปีเกิด | 8 มิถุนายน 2529 |
| วุฒิการศึกษา | ปีการศึกษา 2551: บริหารธุรกิจบัณฑิต (คอมพิวเตอร์ธุรกิจ) มหาวิทยาลัยราชภัฏสวนดุสิต |
| ตำแหน่ง | นักวิชาการคอมพิวเตอร์ |

ผลงานทางวิชาการ

ธีรยุทธ เอกรุณ, และ ณัฐธนนท์ หงส์วริทธิ์ธร. (มิถุนายน 2558). *อิทธิพลของรูปแบบการใส่รหัสผ่านและประเภทของรหัสผ่านต่อการพิสูจน์ตัวตนด้วยรหัสผ่านตัวอักษรร่วมกับการใช้ตารางกริดและรูปภาพ*. การประชุมวิชาการระดับชาติและนานาชาติ คณะวิทยาการจัดการ มหาวิทยาลัยราชภัฏสวนสุนันทา ครั้งที่ 2 (ICMSIT 2015), มหาวิทยาลัยราชภัฏสวนสุนันทา, กรุงเทพฯ.

| | |
|---|---|
| ประสบการณ์ทำงาน | 2555-ปัจจุบัน: นักวิชาการคอมพิวเตอร์ สำนักอำนวยการประจำศาลอุทธรณ์ภาค 7 |
| | 2551-2555: นักวิชาการคอมพิวเตอร์ สำนักอำนวยการประจำศาลอุทธรณ์ภาค 4 |