การศึกษาปัจจัยสำคัญที่มีต่อการสร้างรหัสผ่านรูปภาพแบบกริด

ณัฐธนนท์ หงส์วริทธิ์ธร[1*] และ ดนุพัฒน์ กชชาดาปภาดา[2]

บทคัดย่อ

งานวิจัยชิ้นนี้เป็นการสำรวจถึงปัจจัยในการออกแบบรหัสผ่านรูปภาพแบบกริด เนื่องจากมีปัจจัยที่สำคัญหลายปัจจัยมิได้ถูกกล่าวหรือได้อธิบายไว้ถึงในงานวิจัยที่ผ่านมาว่า ปริมาณหรือรูปแบบที่เหมาะสมของตัวแปรสำหรับการสร้างรหัสผ่านรูปภาพแบบกริด งานวิจัยนี้จึงได้ทำการออกแบบข้อคำถามเพื่อทำการสำรวจความคิดเห็นเกี่ยวกับปัจจัยที่สำคัญในการออกแบบรหัสผ่านรูปภาพแบบกริด โดยผลการสำรวจจากจำนวนผู้ตอบแบบสอบถามออนไลน์ทั้งหมด 423 คน พบว่า ผู้ตอบแบบสอบถามเห็นด้วยกับตารางกริดขนาด 4x4 รูปแบบจัตุรัส รูปภาพสำหรับสร้างรหัสผ่านนั้นควรเป็นรูปภาพประเภทรูปธรรม ซึ่งคะแนนเฉลี่ย 2 อันดับแรกได้แก่ รูปภาพสิ่งมีชีวิตและรูปภาพเหมือนจริง จำนวนไอคอนรูปภาพสำหรับสร้างรหัสผ่านมีทั้งหมด 30 รูป และในขั้นตอนการสร้างรหัสผ่านสามารถเลือกไอคอนรูปภาพซ้ำได้ ผู้ตอบแบบสอบถามเห็นด้วยกับรูปแบบการสร้างรหัสผ่านแบบผู้ใช้งานสร้างเองทั้งหมดมากกว่ารูปแบบที่คอมพิวเตอร์ทำการสร้างรหัสผ่านเริ่มต้นให้ ผู้ตอบแบบสอบถามเห็นด้วยกับรูปแบบปฏิสัมพันธ์ในการสร้างรหัสผ่านเป็นแบบการคลิกเลือกมากกว่าแบบการลากและวาง

นอกจากนี้ได้มีการวิเคราะห์ข้อมูลเพิ่มเติมระหว่างข้อมูลทั่วไปของผู้ตอบแบบสอบถามกับปัจจัยที่ทำการสำรวจซึ่งมีความสัมพันธ์กันหลายปัจจัย โดยจะนำข้อมูลที่ได้จากการสำรวจมาทำการออกแบบงานวิจัยเชิงทดลองเกี่ยวกับรหัสผ่านรูปภาพแบบกริด ที่มีการทดสอบความสมดุลย์กันระหว่างระดับความปลอดภัยกับความง่ายในการจดจำต่อไป

คำสำคัญ: สำรวจ, รหัสผ่านรูปภาพ, รหัสผ่านรูปภาพแบบกริด

[1] ผู้ช่วยศาสตราจารย์ สาขาวิชาวิทยการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์
[2] นักศึกษาปริญญาโท สาขาวิชาวิทยการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธรรมศาสตร์
[*] ผู้นิพนธ์ประสานงาน โทร. 0-2986-9156 ต่อ 229 อีเมล: chcstu@gmail.com

Important Factors for Grid-based Graphical Passwords

Nuttanont Hongwarittorn[1*] and Dhanuphat Kotchadapaphada[2]

Abstract

This research surveys the factors in designing a grid-based graphical password since the previous research on this topic has not been explained or given any reasons why the quantity or form of several important factors are used in much research of grid-based graphical passwords. This study was therefore designed to survey user opinions of important factors in creating grid-based graphical passwords. The survey results showed that respondents agreed that a 4*4 grid should be used to form a password. Images which should be used as passwords were concrete icons. The icons scored in the first two highest were photographs and images respectively. The number of image icons used as password choices were about 30 icons in a grid size of 5*6. Any Icon could be used as passwords repeatedly. Respondents preferred creating passwords by themselves to being generated by a machine; however, Surprisingly, respondents preferred the point and click to the drag and drop interaction style.

In addition to the survey results, the preliminary relations between the factors and user's demographic data were further analyzed. Several significant relations were found. Those survey factors would be further examined in experiments to check how usable and secured.

Keywords: survey, graphical password, Grid-based Graphical Password

---

[1] Assistant Professor, Department of Computer Science Faculty of Science and Technology, Thammasat University

[2] Master's Student in the Master's Degree Program of Computer Science, Department of Computer Science Faculty of Science and Technology, Thammasat University

[*] Corresponding Author Tel. 0-2986-9156 Ext. 229 E-mail: chcstu@gmail.com

1. บทนำ

ปัจจุบันการจะเข้าถึงข้อมูล ที่จัดเก็บไว้ในคอมพิวเตอร์จำเป็นต้องมีการกำหนดสิทธิในการเข้าใช้ระบบ เพื่อป้องกันการเข้าถึงข้อมูลส่วนตัวที่สำคัญและอาจสร้างความเสียหายให้กับเจ้าของข้อมูลได้ ตัวอย่างเช่นการเข้าใช้งานอีเมล (E-mail) โซเชียลเน็ตเวิร์ค (Social Network) หรือการเข้าใช้งานคอมพิวเตอร์ส่วนบุคคล ดังนั้นการที่จะเข้าถึงข้อมูล จำเป็นต้องผ่านวิธีการพิสูจน์ตัวตน เพื่อเป็นการยืนยันตัวตนและป้องกันปัญหาเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล ซึ่งวิธีการพิสูจน์ตัวตนที่เป็นที่นิยมและมีการใช้งานอย่างแพร่หลายคือวิธีการพิสูจน์ตัวตนโดยใช้ตัวอักษรแทนชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเป็นการยืนยันว่าบุคคลต้องการเข้าถึงข้อมูลเป็นผู้มีสิทธิเข้าถึงข้อมูล อย่างไรก็ตามก็ยังมีบุคคลบางกลุ่มที่เป็น นักเลงคอมพิวเตอร์ (Hacker) ที่มีความชำนาญทางด้านคอมพิวเตอร์ พยายามทำการเข้าถึงข้อมูลของบุคคลอื่น ดังนั้นจึงมีงานวิจัยเกี่ยวกับวิธีการพิสูจน์ตัวตนที่มีการพัฒนาออกมาอย่างต่อเนื่อง เพื่อให้สามารถใช้งานได้ง่าย (Usability) และมีความปลอดภัยสูง (Security) โดยงานวิจัยเกี่ยวกับการพิสูจน์ตัวตน ที่มีการวิจัยกันอย่างแพร่หลาย คืองานวิจัยเกี่ยวกับรหัสผ่านรูปภาพ (Graphical Password)

รูปที่ 1 ตัวอย่างขนาดรูปภาพจากงานวิจัย [1], [2]

จากรูปที่ 1 เป็นตัวอย่างรหัสผ่านรูปภาพที่มีปริมาณรูปภาพมากมาย ถึงแม้ว่าจำนวนของภาพที่จะถูกเลือกมาเป็นรหัสผ่านจะขึ้นอยู่กับรูปแบบการสร้างรหัสผ่านรูปภาพ แต่การสร้างรหัสผ่านรูปภาพหลายชิ้น ที่มีลักษณะที่ผู้ใช้ต้องเลือกรูปภาพมาใส่ในตารางกริดจำนวนของรูปภาพที่จะเป็นตัวเลือกให้กับผู้ใช้สร้างรหัสผ่าน จึงเป็นปัจจัยสำคัญต่อผู้ใช้ที่ต้องจดจำและระดับความปลอดภัยของรหัสผ่านด้วย อย่างไรก็ตามปัจจัยทางด้านนี้ยังไม่ได้ถูกอธิบายไว้ในงานวิจัยรหัสผ่านรูปภาพอย่างชัดเจน

รูปที่ 2 ตัวอย่างการตั้งรหัสผ่านรูปภาพที่เลือกภาพติดกัน

ในการตั้งรหัสผ่านแบบตัวอักษร ผู้ใช้งานมักตั้งรหัสผ่านที่ง่ายต่อการจดจำ ทำให้รหัสผ่านนั้นไม่ผ่านกฎเกณฑ์การสร้างรหัสผ่าน เพื่อให้ได้รหัสผ่านที่มีความปลอดภัยสูง ระบบคอมพิวเตอร์หลายระบบจึงมีการแนะนำวิธีการตั้งรหัสผ่านเพื่อให้ได้รหัสผ่านที่มีความปลอดภัยที่สูงขึ้นเช่น มีการระบุจำนวนของตัวอักษรต้องมีขนาด 8 ตัวอักษร รหัสผ่านต้องผสมกันระหว่าง ตัวเลข ตัวอักษรและสัญลักษณ์ หรือในบางระบบมีการตั้งรหัสผ่านให้กับผู้ใช้ซึ่งโดยปกติแล้วรหัสผ่านที่สร้างขึ้นจะมีรูปแบบที่ยากต่อการจดจำ แต่ผู้ใช้ก็สามารถปรับแก้ให้ง่ายขึ้นได้ภายหลัง เป้าหมายสำคัญของงานวิจัยในด้านรหัสผ่านคือต้องการได้รหัสผ่านที่ง่ายต่อการจดจำ แต่ยากต่อผู้ที่ไม่หวังดีที่พยายามจะลักลอบขโมยจดจำรหัสผ่าน จึงเป็นเรื่องที่ควรทำการศึกษาต่อไปที่ระบบคอมพิวเตอร์ในการสร้างรหัสผ่านรูปภาพ ควรที่ต้องตรวจสอบรหัสผ่านรูปภาพที่ผู้ใช้สร้างขึ้นมีระดับความปลอดภัยมากน้อยเพียงใด และเมื่อระบบตรวจสอบรหัสผ่านรูปภาพแล้วว่า รหัสผ่านรูปภาพที่ผู้ใช้สร้างดังตัวอย่างเช่นการสร้างรหัสผ่านในรูปที่ 2 มีการสร้างรหัสผ่านติดกันทั้งหมด 5 ตำแหน่งซึ่งจะมีความปลอดภัยต่ำ ระบบควรจะสร้างหรือมีส่วนร่วมในการสร้างรหัสผ่านรูปภาพให้ผู้ใช้หรือไม่ ระบบควรมีกลไกเพื่อช่วยในการตั้งรหัสผ่านรูปภาพ เพื่อให้เกิดรหัสผ่านที่มีระดับความปลอดภัยที่สูงขึ้นเหมือนอย่างกับการตั้งรหัสผ่านแบบตัวอักษร โดยอาจอยู่ในรูปแบบที่คอมพิวเตอร์ทำการตั้งรหัสผ่านให้ทั้งหมดหรืออาจผสมกันระหว่างคอมพิวเตอร์ตั้งให้บางส่วนและผู้ใช้งานตั้งเองบางส่วน ผู้ใช้จะมี

ความคิดเห็นอย่างไรต่อรหัสผ่านที่ถูกสร้างขึ้นในลักษณะนี้ งานวิจัยจึงได้สำรวจความคิดของผู้ใช้ในประเด็นนี้ด้วย

ในกระบวนการพิสูจน์ตัวตนด้วยรหัสผ่านรูปภาพ การออกแบบส่วนต่อประสาน (User Interface) ในการสร้างและใช้รหัสผ่านรูปภาพ เป็นประเด็นสำคัญอีกประเด็นหนึ่ง เพราะวิธีที่ผู้ใช้สร้างรหัสผ่านและใช้รหัสผ่านเพื่อเข้าสู่ระบบ มีความสัมพันธ์กับการจดจำรหัสผ่านของผู้ใช้และความปลอดภัยด้วย เช่นระหว่างส่วนต่อประสานแบบการกดเลือกกับการกดลากภาพที่ต้องการใช้เป็นรหัสผ่าน ส่วนต่อประสานในการสร้างและใช้รหัสผ่านน่าจะส่งผลต่อผู้ใช้ที่แตกต่างกัน เช่นผู้ใช้ที่เป็นเด็ก ผู้ใช้ที่เป็นผู้สูงอายุ รูปแบบการปฏิสัมพันธ์ในการสร้างและใช้รหัสผ่านรูปภาพ ได้สำรวจในงานวิจัยนี้ด้วย

เนื่องจากในการทำการวิจัยเชิงการทดลอง ผู้วิจัยต้องเลือกศึกษาปัจจัยหรือตัวแปรบางตัว และต้องให้ตัวแปรบางตัวแปรคงที่เอาไว้ จึงเป็นเรื่องยากและจะทำให้การทดลองมีระดับความซับซ้อน งานวิจัยจึงเริ่มศึกษาสำรวจปัจจัยที่ผู้ใช้เห็นด้วยมากน้อย เพื่อนำเอาไปเป็นจุดเริ่มต้นในการสร้างรหัสผ่านรูปภาพได้ ประเด็นหลักสำคัญที่จะได้ถูกสำรวจได้แก่ ขนาดและรูปแบบของตารางกริด ประเภทของรูปภาพ ขนาดและจำนวนของรูปภาพ รูปแบบการได้มาของรหัสผ่านรูปภาพ และรูปแบบปฏิสัมพันธ์ในขั้นตอนการสร้างรหัสผ่าน โดยรายละเอียดของงานวิจัยในส่วนถัดไปจะกล่าวถึงส่วนที่ 2 ระเบียบวิธีวิจัย ส่วนที่ 3 ผลการสำรวจ ส่วนที่ 4 สรุปและอภิปรายผล

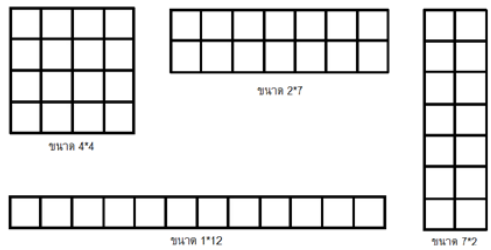
2. ระเบียบวิธีการศึกษาวิจัย

การวิจัยในครั้งนี้ใช้รูปแบบการวิจัยเชิงสำรวจ (Survey Research) โดยการใช้แบบสอบถามออนไลน์เป็นเครื่องมือช่วยในการทำวิจัย เพื่อสำรวจถึงปัจจัยที่ใช้ในการออกแบบรหัสผ่านรูปภาพแบบกริดที่ผู้ใช้เห็นด้วยมากที่สุด

2.1 ปัจจัยในการสำรวจ

การวิจัยในครั้งนี้เป็นงานวิจัยที่ต้องการศึกษาถึงปัจจัยที่สำคัญต่อการออกแบบรหัสผ่านรูปภาพแบบกริดโดยใช้วิธีวิจัยเชิงสำรวจ (Survey Research) ด้วยแบบสอบถามออนไลน์ เพื่อประมวลข้อคิดเห็นจากผู้ใช้ที่มีปัจจัยตามที่ได้อธิบายไปแล้วนั้น มาเป็นพื้นฐานในการออกแบบรหัสผ่านรูปภาพแบบกริด ที่น่าจะตรงกับความต้องการของผู้ใช้ได้มากที่สุด

ในการออกแบบรหัสผ่านรูปภาพแบบกริด ในงานวิจัยที่ผ่านมาไม่พบงานวิจัยใดที่ได้ระบุไว้อย่างชัดเจนในส่วนของปัจจัยต่าง ๆ ที่นำมาออกแบบรหัสผ่านรูปภาพแบบกริด ดังนั้นงานวิจัยชิ้นนี้โดยแบ่งตามปัจจัยดังต่อไปนี้



รูปที่ 3 แสดงขนาดและรูปแบบของตารางกริดสำหรับนำมาใช้สร้างรหัสผ่านรูปภาพแบบกริด

ปัจจัยที่หนึ่ง งานวิจัยที่ผ่านมาได้มีการกำหนดขนาดของกริดที่แตกต่างกัน เช่น ขนาด 3*5 [3], ขนาด 6*6 [4], [5], ขนาด 3*3 [1], [6] และขนาด 5*5 [7] เป็นต้น แต่ไม่พบงานวิจัยใดที่ได้ระบุชัดเจนว่าทำไม่ถึงใช้ขนาดดังกล่าว ดังนั้นงานวิจัยชิ้นนี้จึงทำการสำรวจขนาดและรูปแบบของตารางกริดที่เหมาะสมสำหรับการนำมาสร้างรหัสผ่านรูปภาพแบบกริด โดยขนาดของตารางกริดที่มีขนาดใหญ่หรือจำนวนช่องที่มาก ซึ่งทำให้ได้รหัสผ่านที่หลากหลายเพิ่มมากขึ้นและช่วยให้รหัสผ่านมีความปลอดภัยเพิ่มขึ้น แต่ผู้ใช้งานอาจไม่สะดวกในการจดจำ และหากมีขนาดที่กว้างหรือลึกมาก ก็อาจส่งผลต่อความยากง่ายในการใช้งานของผู้ใช้งาน เนื่องจากผู้ใช้งานอาจต้องทำการกวาดสายตาในการใช้งาน ดังนั้น ในงานวิจัยชิ้นนี้ได้สำรวจตารางกริดที่มีขนาดและรูปแบบที่แตกต่างกัน 4 ขนาด ได้แก่ ตารางขนาด 4*4 รูปแบบจัตุรัส เป็นรูปแบบที่ผู้ใช้งานไม่จำเป็นต้องกวาดสายตาในการมองและตารางขนาด 2*7, 7*2 และ 1*12 รูปแบบผืนผ้า เป็นรูปแบบแนวกว้างหรือแนวยาวที่ ผู้ใช้ต้องทำการกวาดสายตาไปทางด้านใดด้านหนึ่ง ดังรูปที่ 3 ซึ่งเป็นตัวอย่างที่ได้ทำการออกแบบสำหรับเป็นตัวเลือกในแบบสอบถามซึ่งเป้าหมายของตัวเลือกเพื่อต้องการให้ผู้ตอบแบบสอบถามเห็นลักษณะของรูปทรงของตารางกริด มิได้ต้องการเปรียบเทียบจำนวนของเซลล์ (Cell) โดยตรงเนื่องจากมี

ความหลากหลาย โดยกำหนดให้ขนาดของตัวเลือกทั้ง 4 ขนาด มีขนาดใกล้เคียงกันมากที่สุด ซึ่งหากผู้ตอบแบบสอบถามเห็นว่ามีขนาดอื่นที่เหมาะสมก็สามารถทำการระบุเพิ่มเติมได้ ซึ่งงานวิจัยที่ผ่านมาส่วนมากใช้เป็นรูปแบบจัตุรัสมากกว่ารูปแบบผืนผ้า นอกเหนือจากการกวาดสายตาอาจมีข้อจำกัดในเรื่องของหน้าจอที่ใช้ในการสร้างรหัสผ่านรูปภาพที่มีขนาดที่จำกัดหรือต้องการจำกัดเนื้อที่ให้อยู่ในบริเวณที่ไม่ควรจะใหญ่เกินไปหรือใช้เนื้อที่มากเกินไป ตารางกริดรูปแบบจัตุรัสน่าจะเป็นรูปแบบที่ผู้ตอบแบบสอบถามเห็นด้วยหากนำมาใช้สร้างรหัสผ่านรูปภาพ

รูปที่ 4 แสดงประเภทของรูปภาพสำหรับนำมาใช้สร้างรหัสผ่านรูปภาพ

ปัจจัยที่สอง จากงานวิจัยที่ผ่านมาได้ใช้รูปภาพประเภทที่แตกต่างกันเช่น ภาพหน้าคน [1], [5] ภาพประเภทนามธรรม [3], [8] และใช้ภาพที่ผสมกันระหว่างสัญลักษณ์และรูปสัตว์ [2] ภาพที่นำมาใช้มีหลายชนิดและหลายประเภท จึงอาจส่งผลต่อความรู้สึกของผู้ใช้งานในการจดจำ งานวิจัยนี้จึงสำรวจประเภทของรูปภาพสำหรับเป็นตัวเลือกในการสร้างรหัสผ่านรูปภาพ (Graphical Password) เพื่อสำรวจว่ารูปภาพประเภทใดอาจช่วยเพิ่มความรู้สึกที่ง่ายต่อการจดจำของผู้ใช้งาน ประเภทของรูปภาพถูกแบ่งออกเป็น 2 ประเภทใหญ่ ดังต่อไปนี้ 1) รูปภาพประเภทรูปธรรม ได้แก่ รูปภาพวัตถุ รูปวาดเหมือนจริง เช่นรูปบ้าน รูปรถ รูปการ์ตูน รูปวาด เป็นต้น 2) รูปภาพประเภทนามธรรม ได้แก่รูปภาพที่ไม่สามารถบอกความหมายของรูปดังกล่าวได้เช่น รูปลายเส้นสี ดังรูปที่ 4 จากงานวิจัยรหัสผ่านรูปภาพที่ผ่านมาจะเห็นได้ว่าใช้รูปภาพที่เป็นประเภทรูปธรรมเป็นส่วนใหญ่ ซึ่งอาจเป็นความจริงที่ว่ารูปภาพประเภทนามธรรมเป็นรูปภาพที่ยากต่อการจดจำ เนื่องจากเป็นรูปภาพที่มีรายละเอียดมากและผู้ใช้อาจไม่สามารถให้ชื่อกับรูปภาพนั้นได้เมื่อเทียบกับรูปภาพวัตถุที่ผู้ใช้สามารถเรียกภาพนั้นได้ จึงอาจสันนิษฐานได้ว่าผู้ใช้น่าจะเห็นด้วยที่รูปภาพประเภทรูปธรรมจะถูกนำมาใช้สร้างเป็นรหัสผ่านมากกว่ารูปภาพประเภทนามธรรม ในการสำรวจครั้งนี้ได้ทำการแบ่งรูปภาพประเภทรูปธรรมออกเป็น 5 ชนิด 1) รูปภาพวัตถุ เช่น รูปบ้าน, รูปรถ 2) รูปภาพเหมือนจริงเช่น รูปการ์ตูน, รูปวาด 3) รูปภาพถ่ายที่ไม่ใช้วัตถุเช่น รูปสถานที่ท่องเที่ยว, รูปวิวทิวทัศน์ 4) รูปภาพสิ่งมีชีวิตเช่น รูปคน, รูปสัตว์ 5) รูปภาพบุคคลที่มีชื่อเสียงเช่น รูปดารา, รูปนักร้อง รูปภาพเหมือนจริงและรูปภาพวัตถุน่าจะเป็นประเภทที่มีผู้ตอบแบบสอบถามเลือกมากที่สุดจาก 5 ชนิด เนื่องจากเป็นประเภทของรูปภาพที่ผู้ตอบแบบสอบถามเจอในชีวิตประจำวัน

รูปที่ 5 แสดงจำนวนภาพสำหรับสร้างรหัสผ่านรูปภาพ

ปัจจัยที่สาม งานวิจัยเลือกใช้จำนวนรูปภาพเป็นรหัสผ่านที่มีจำนวนมากน้อยที่แตกต่างกัน เช่น มีการสุ่มจำนวนภาพมาให้เลือกเป็นรหัสผ่าน 100 ภาพ [2], ใช้ภาพ 15 ภาพ [3] และที่ใช้ภาพครั้งละ 9 ภาพ [1] โดยจำนวนภาพไอคอนย่อมส่งผลต่อการจดจำของผู้ใช้งาน หากมีจำนวนรูปภาพมากผู้ใช้งานอาจเกิดความสับสนและอาจทำให้ผู้ใช้งานรู้สึกยากในการจดจำ แต่น่าส่งผลดีในเรื่องของความปลอดภัยที่สูงขึ้น ในทำนองกลับกันหากมีจำนวนรูปภาพน้อยเกินไปน่าส่งผลในเรื่องของความหลากหลายของรหัสผ่านทำให้ได้รหัสผ่านที่มีความปลอดภัยที่ต่ำลง แต่ผู้ใช้งานสามารถใช้งานได้ง่าย เพื่อต้องการทราบจำนวนที่เหมาะสมของรูปภาพที่จะใช้เป็นตัวเลือกสำหรับสร้างรหัสผ่าน การสำรวจครั้งนี้จึงทำการสำรวจจำนวนภาพที่เหมาะสมในการนำมาใช้เป็นตัวเลือกสำหรับสร้างรหัสผ่าน จำนวนของไอคอนรูปภาพแบ่งออกเป็น 3 ระดับ 1) จำนวน 30 รูป โดยใช้รูปภาพที่เป็น

ภาพวัตถุ ผสมกันระหว่างรูปบ้านและรูปรถ โดยมีจำนวนภาพที่น้อยซึ่งช่วยผู้ใช้งานในเรื่องของการจดจำที่ง่ายขึ้น แต่ส่งผลต่อความหลากหลายของรหัสผ่านที่มีความปลอดภัยต่ำลง 2) จำนวน 64 รูป และ 3) จำนวน 100 รูป โดยใช้รูปวาดเหมือนจริง ที่เป็นรูปภาพแสดงอารมณ์ (Emoticon) และรูปการ์ตูน ตามลำดับ ทั้ง 2 แบบมีจำนวนรูปภาพที่เพิ่มขึ้นจากแบบที่ 1 ซึ่งช่วยเพิ่มความหลากหลายของรหัสผ่าน ทำให้มีความปลอดภัยเพิ่มขึ้น แต่ผู้ใช้งานต้องจดจำมากขึ้นเช่นกัน ดังรูปที่ 5 เป็นรูปแบบตัวอย่างของจำนวนรูปภาพที่ได้ทำการออกแบบเป็นรูปแบบจัตุรัสเพื่อให้ผู้ตอบแบบสอบถามสามารถมองและทราบถึงจำนวนของรูปภาพที่จะนำใช้เป็นตัวเลือกในการสร้างรหัสผ่านได้ง่ายขึ้นว่าจะใช้จำนวนเท่าไร ซึ่งในการออกแบบคาดว่าผู้ใช้งานเลือกรูปแบบของขนาดที่มีจำนวนน้อยที่สุดคือขนาด 5x6 เนื่องจากผู้ใช้งานอาจไม่อยากจดจำภาพจำนวนมาก

ปัจจัยที่สี่ จากงานวิจัยที่ผ่านมาพบว่าในการตั้งรหัสผ่านแบบตัวอักษร (Text-Password) ผู้ใช้งานตั้งรหัสผ่านที่ง่ายและใช้รหัสผ่านเดียวกันในหลายระบบเพื่อให้ง่ายขึ้นในการจดจำ แต่วิธีการดังกล่าวมิได้เป็นวิธีการที่ดีและมีความเสี่ยงสูง โดยเฉพาะถ้ารหัสผ่านได้ถูกโจรกรรมไปได้ เพื่อเพิ่มความปลอดภัยที่สูงขึ้น ระบบจึงมีกฎเกณฑ์ที่ช่วยให้ผู้ใช้งานตั้งรหัสผ่านที่มีความปลอดภัยที่สูงขึ้น เช่นมีการระบุจำนวนของตัวอักษรต้องมีขนาด 8 ตัวอักษร รหัสผ่านต้องผสมกันระหว่างตัวเลข ตัวอักษรและสัญลักษณ์ หรือระบบอาจสร้างรหัสผ่านให้ผู้ใช้ ซึ่งน่าจะยากต่อการจดจำ ดังนั้น ในการสร้างรหัสผ่านรูปภาพระบบควรกำหนดกฎเกณฑ์ที่ช่วยผู้ใช้ในการตั้งรหัสผ่านรูปภาพเพื่อให้ได้รหัสผ่านรูปภาพที่มีความปลอดภัยที่สูงขึ้น ซึ่งอาจใช้วิธีการสร้างรหัสผ่านรูปภาพแบบคอมพิวเตอร์สร้างรหัสผ่านรูปภาพให้ทั้งหมดหรือสร้างบางส่วน ผู้ใช้จะมีความคิดเห็นต่อรหัสผ่านแบบนี้อย่างไร ในการสำรวจจึงได้แบ่งการได้รหัสผ่านเป็น 3 วิธี 1) คอมพิวเตอร์สร้างรหัสผ่านรูปภาพให้ทั้งหมด 2) คอมพิวเตอร์สร้างให้บางส่วนและผู้ใช้งานสร้างเองบางส่วนและ 3) ผู้ใช้งานสร้างรหัสผ่านเองทั้งหมด

ปัจจัยที่ห้า ในการสร้างรหัสผ่านรูปภาพ รูปแบบของส่วนต่อประสานย่อมส่งผลต่อผู้ใช้ในการสร้างและใช้งานรหัสผ่านทั้งในแง่ความสะดวกและความปลอดภัย ตลอดจนความแตกต่างของกลุ่มผู้ใช้งาน ไม่ว่าจะเป็นความแตกต่างในอายุ เพศ หรือในด้านอื่นด้วย ดังนั้นงานวิจัยชิ้นนี้ได้สำรวจรูปแบบปฏิสัมพันธ์ในขั้นตอนการสร้างรหัสผ่านรูปภาพหรือการพิสูจน์ตัวตน ควรมีรูปแบบอย่างไร ที่ผู้ใช้คิดว่ามีความสะดวกในการใช้งานและอาจช่วยป้องกันการถูกโจรกรรม โดยแบ่งออกเป็น 2 รูปแบบดังนี้ 1) แบบ Drag and Drop คือการคลิกไอคอนรูปภาพค้างไว้และทำการลากไปยังจุดที่ต้องการในตารางกริดรหัสผ่านและทำการปล่อยเมาส์ (Mouse) เป็นรูปแบบที่ช่วยให้ผู้ใช้มีความสะดวกขึ้นในการใช้งานเพราะมีการคลิกเพียงครั้งเดียว 2) แบบ Point and Click คือการคลิกเลือกไอคอนรูปภาพที่ต้องการ 1 ครั้ง และทำการคลิกเลือกจุดที่ต้องการในตารางกริดรหัสผ่านเพื่อวางไอคอนรูปภาพอีก 1 ครั้ง เป็นวิธีที่อาจช่วยป้องกันความปลอดภัยจากการโจรกรรมเนื่องจากขณะทำการคลิกผู้ที่ต้องการโจรกรรมอาจมองไม่ทันว่าคลิกเลือกที่ภาพใด และนอกจากนั้นยังสำรวจถึงวิธีเลือกรูปภาพในตอนสร้างรหัสผ่าน ซึ่งแบ่งออกเป็น 2 วิธีการคือ 1) รูปภาพสามารถถูกเลือกซ้ำได้ ซึ่งวิธีการนี้ช่วยเพิ่มตัวเลือกของรหัสผ่านที่เพิ่มขึ้น แต่ก็อาจส่งผลต่อความปลอดภัยที่ต่ำลง หากผู้ใช้งานเลือกใช้รูปเดิมหรือ 2) รูปภาพห้ามถูกใช้ซ้ำเป็นวิธีการที่จะได้รหัสผ่านรูปภาพที่มีรูปภาพที่แตกต่างกันจึงทำให้มีความปลอดภัยเพิ่มขึ้น แต่ผู้ใช้งานต้องจดจำรูปภาพเพิ่มขึ้นเช่นกัน

2.2 ประชากรกลุ่มตัวอย่าง

งานวิจัยนี้เป็นการสำรวจเพื่อหาปัจจัยในการออกแบบรหัสผ่านรูปภาพแบบกริด โดยได้ทำการสำรวจกับกลุ่มผู้ใช้งานอินเทอร์เน็ตทั่วไป โดยได้ทำการโพสแบบสอบถามออนไลน์ผ่านช่องทางเว็บไซต์ดังต่อไปนี้ www.facebook.com, www.pantip.com, www.mthai.com และ www.blognone.com โดยเป็นการเชิญชวนให้มาร่วมทำแบบสอบถาม

2.3 เครื่องมือที่ใช้ในงานวิจัย

เครื่องมือที่ใช้ในงานวิจัยคือแบบสอบถามออนไลน์ โดยต้องทำการระบุทุกข้อคำถามของแบบสอบถาม เพื่อเป็นการป้องกันข้อมูลที่ไม่สมบูรณ์ ซึ่งเนื้อหาของแบบสอบถามแยกออกเป็น 3 ส่วนดังนี้ 1) เป็นข้อคำถามเกี่ยวกับ ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม 2) เป็นข้อ

คำถามเกี่ยวกับความคิดเห็นที่มีต่อการสร้างรหัสผ่าน (Password) 3) เป็นข้อคำถามเกี่ยวกับความคิดเห็นที่มีต่อรหัสผ่านรูปภาพ (Graphical Password)

2.4 ผลการวิเคราะห์ข้อมูล

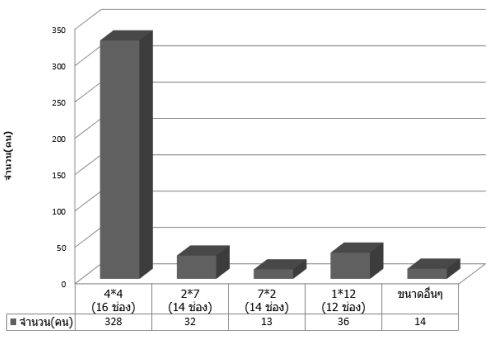
การวิเคราะห์ข้อมูลในงานวิจัยครั้งนี้ ผู้วิจัยได้ทำการแบ่งการวิเคราะห์ข้อมูลออกเป็น 3 ส่วน ส่วนที่หนึ่งเป็นการสรุปผลข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ส่วนที่สองเป็นการสรุปผลตามปัจจัยหรือตัวแปรสำคัญที่ต้องการสำรวจและส่วนสุดท้ายเป็นการสรุป วิเคราะห์เพิ่มเติม

3. ผลการสำรวจ

3.1 ข้อมูลทั่วไป

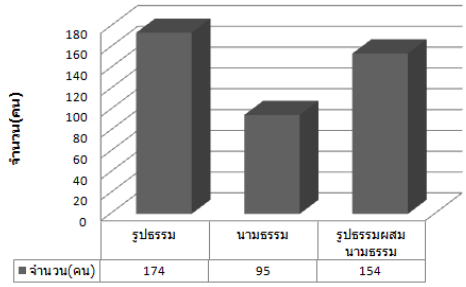
โดยจากการสำรวจช่วงเวลาตั้งแต่วันที่ 19 กรกฎาคม 2556 ถึงวันที่ 10 สิงหาคม 2556 พบว่า ข้อมูลทั่วไปของผู้ตอบแบบสอบถามที่ตอบแบบสอบถามทั้งหมด 423 คน เป็นเพศชายร้อยละ 58.63 และเพศหญิงร้อยละ 41.37 มีผู้ตอบแบบสอบถามจำนวน 280 คน รู้จักรหัสผ่านรูปภาพ อายุส่วนใหญ่ของผู้ตอบแบบสอบถามอยู่ในช่วง 21-30 ปี ระดับการศึกษาส่วนใหญ่เป็นระดับปริญญาตรี กลุ่มอาชีพที่ตอบแบบสอบถามมากที่สุดคือพนักงานบริษัทเอกชน และในจำนวนนั้นมีผู้ตอบแบบสอบถามอยู่ 188 คนที่เคยใช้งานรหัสผ่านรูปภาพมาแล้ว โดยทั่วไปผู้ตอบแบบสอบถามร้อยละ 38 ระบุว่าไม่ค่อยลืมรหัสผ่านและผู้ตอบแบบสอบถามร้อยละ 11 ไม่เคยลืมรหัสผ่าน

3.2. สรุปผลตามปัจจัยของงานวิจัย



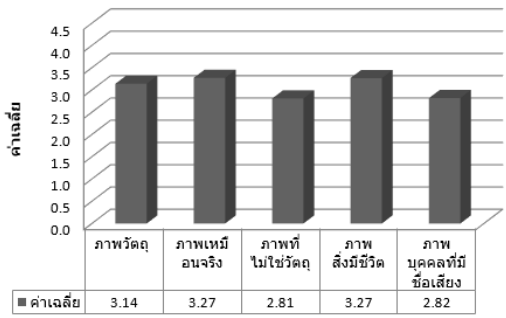
รูปที่ 6 ความถี่ของผู้ตอบแบบ สอบถามเกี่ยวกับขนาดของตารางกริด (Grid) สำหรับการสร้างรหัสผ่านรูปภาพ

จากรูปที่ 6 ชี้ให้เห็นว่า 77.54% ของผู้ตอบแบบสอบถาม เห็นด้วยที่จะใช้ตารางกริดขนาด 4x4 ซึ่งเป็นรูปแบบจัตุรัส ในการสร้างรหัสผ่านรูปภาพ 8.51% ของผู้ตอบแบบสอบถามกับเห็นด้วยกับตารางกริดขนาด 1*12 และตารางกริดขนาด 7*2 เป็นตารางขนาดที่มีจำนวนผู้ตอบแบบสอบถามเห็นด้วยน้อยที่สุดในการใช้สร้างรหัสผ่านรูปภาพ



รูปที่ 7 ความถี่ของประเภทของรูปภาพที่จะนำมาใช้เป็นตัวเลือกในการสร้างรหัสผ่าน

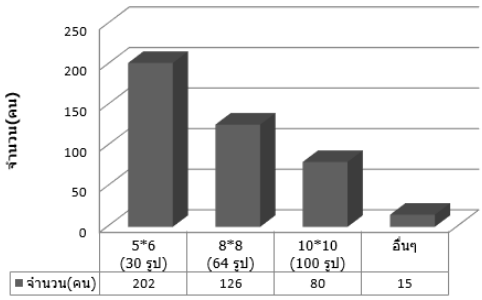
รูปที่ 7 เป็นการแสดงให้เห็นผลสำรวจประเภทของรูปภาพที่นำมาใช้เป็นตัวเลือกในการสร้างรหัสผ่าน ผู้ตอบแบบสอบถาม 41.13% เห็นด้วยที่จะนำเอารูปภาพประเภทรูปธรรมมาใช้สร้างเป็นรหัสผ่าน รองลงมาคือ 36.41% ผสมกันระหว่างรูปธรรมและนามธรรม



รูปที่ 8 ค่าเฉลี่ยในการสำรวจชนิดของรูปภาพที่

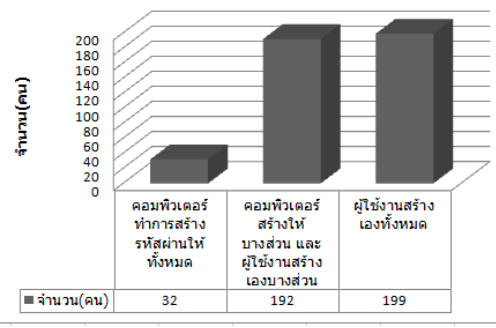
นำมาใช้เป็นตัวเลือกสำหรับสร้างรหัสผ่าน การสำรวจเกี่ยวกับชนิดของรูปภาพรูปธรรมที่ควรนำมาใช้เป็นรหัสผ่าน รูปที่ 8 แสดงให้เห็นว่า รูปภาพที่ผู้ตอบแบบสอบถามเลือกมากที่สุด 2 อันดับแรกคือ ภาพสิ่งมีชีวิตและภาพเหมือนจริง มีค่าเฉลี่ยเท่ากันทั้ง 2 ประเภทคือเท่ากับ 3.27 ซึ่งภาพรูปธรรมที่ผู้ตอบแบบสอบถามเลือกมีค่าที่ไม่

แตกต่างกัน อาจจะเกิดจากที่ผู้ตอบแบบสอบถามไม่ได้มีความชอบรูปภาพประเภทดังกล่าวอย่างชัดเจน แต่ที่น่าจะเห็นความแตกต่างที่ชัดเจนคือผู้ตอบแบบสอบถามน่าจะชอบภาพที่แบบรูปธรรมมากกว่าภาพแบบนามธรรม



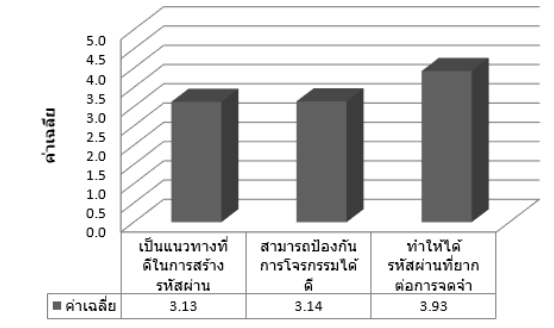
รูปที่ 9 ความถี่ของผู้ตอบแบบสอบถามเกี่ยวกับจำนวนไอคอนรูปภาพ

รูปที่ 9 แสดงถึงผลการสำรวจในปัจจัยจำนวนไอคอนรูปภาพที่ควรใช้เป็นตัวเลือกในตอนสร้างรหัสผ่านรูปภาพ 47.75% ของผู้ตอบแบบสอบถามเห็นด้วยกับตารางขนาด 5*6 (จำนวน 30 รูปภาพ) และ อีก 29.79% ของผู้ตอบแบบสอบถามเห็นด้วยกับตารางขนาด 8*8 (จำนวน 64 ภาพ) และมีจำนวนผู้ตอบแบบสอบถามน้อยลงที่เห็นว่าควรใช้ตารางขนาดใหญ่ขนาด 10*10 (จำนวน 100 ภาพ) หรือ ตารางขนาดอื่น ๆ ที่มีขนาดเล็กเช่น ตาราง 4*3 และ 4*5 ที่มีจำนวนภาพเพียง 12 และ 20 ภาพตามลำดับเท่านั้น



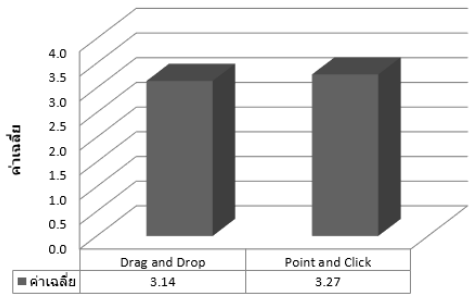
รูปที่ 10 ความถี่ของผู้ตอบแบบสอบถามเกี่ยวกับวิธีการสร้างรหัสผ่านรูปภาพ

รูปที่ 10 แสดงผลการสำรวจปัจจัยพฤติกรรมในการสร้างรหัสผ่านรูปภาพ 47% ของผู้ตอบแบบสอบถาม เห็นด้วยที่ให้ผู้ใช้งานสร้างรหัสผ่านเองทั้งหมดและรองลงมาคือ 45.4% ของผู้ตอบแบบสอบถามเห็นว่าควรให้คอมพิวเตอร์ทำการสร้างรหัสผ่านรูปภาพเริ่มต้นให้บางส่วนและผู้ใช้งานสร้างเองบางส่วน



รูปที่ 11 ค่าเฉลี่ยของข้อคิดเห็นที่มีต่อรหัสผ่านที่สร้างโดยคอมพิวเตอร์ทั้งหมด

การสำรวจครั้งนี้ยังได้มีข้อคำถามที่จะให้ผู้ตอบแบบสอบถามได้ข้อคิดเห็นที่มีต่อรหัสผ่านที่คอมพิวเตอร์เป็นผู้สร้างรหัสผ่านให้ทั้งหมดดังรูปที่ 11 ผู้ตอบแบบสอบถามไม่คิดว่าการให้คอมพิวเตอร์สร้างรหัสผ่านให้ทั้งหมดเป็นการช่วยสร้างรหัสผ่าน ($\bar{x}$ = 3.13, S.D. = 1.089) และไม่แน่ใจว่าเป็นวิธีที่สามารถป้องกันการโจรกรรมได้ดี ($\bar{x}$ = 3.14, S.D. = 1.046) แต่แน่ใจว่ารหัสผ่านที่คอมพิวเตอร์สร้างให้จะยากต่อการจดจำ ($\bar{x}$ = 3.93, S.D. = 1.091)



รูปที่ 12 ข้อมูลผู้ตอบแบบสอบถามเกี่ยวกับรูปแบบปฏิสัมพันธ์ในขั้นตอนการสร้างรหัสผ่านและพิสูจน์ตัวตน

รูปที่ 12 แสดงผลการสำรวจปัจจัยรูปแบบของปฏิสัมพันธ์ในขั้นตอนการสร้างรหัสผ่านหรือการพิสูจน์ตัวตน ผู้ตอบแบบสอบถามเห็นด้วยกับรูปแบบปฏิสัมพันธ์แบบ Point and Click มากกว่า แบบ Drag-Drop และในการสำรวจข้อคิดเห็นว่ารูปภาพที่เป็นตัวเลือกควรจะถูก

นำมาใช้ซ้ำเป็นรหัสผ่านรูปภาพหรือไม่ มีจำนวนผู้ตอบแบบสอบถามถึง 75.4% เห็นว่า สามารถรหัสผ่านที่มีรูปภาพซ้ำกันได้

3.3. วิเคราะห์เพิ่มเติม

ข้อมูลจากการสำรวจครั้งนี้ ได้ถูกนำมาวิเคราะห์เพิ่มเติมเพื่อศึกษาถึงความสัมพันธ์ของข้อมูลส่วนตัวของผู้ตอบแบบสอบถามกับปัจจัยสำคัญต่อการออกแบบและสร้างรหัสผ่าน จากการวิเคราะห์ความสัมพันธ์ โดยใช้การทดสอบไคสแควร์ (Chi-square Test) พบว่ามีความสัมพันธ์กันดังต่อไปนี้

(1) เพศและรหัสผ่านแบบคอมพิวเตอร์สร้างให้จะช่วยป้องกันการโจรกรรมได้ดี มีความสัมพันธ์กันอย่างมีนัยสำคัญทางสถิติ ผลการวิเคราะห์ (Pearson Chi-Square มีค่าเท่ากับ 14.667 df = 4 Sig = .005) ชี้ให้เห็นว่า เพศหญิงและเพศชายมีความคิดเห็นต่อรหัสผ่านแบบคอมพิวเตอร์สร้างให้จะช่วยป้องกันการโจรกรรมได้ดีแตกต่างกัน ผู้ตอบแบบสอบถามเพศชายเห็นด้วยว่ารหัสผ่านที่คอมพิวเตอร์สร้างให้สามารถป้องการโจรกรรมได้ดี มากกว่าผู้ตอบแบบสอบถามเพศหญิง

(2) เพศและรหัสผ่านที่คอมพิวเตอร์สร้างให้จะยากต่อการจดจำ มีความสัมพันธ์กันอย่างมีนัยสำคัญทางสถิติ ผลการวิเคราะห์ (Person Chi-Square มีค่าเท่ากับ 14.667 df = 4 Sig = .005) ชี้ให้เห็นว่าเพศชายและเพศหญิงมีความคิดเห็นต่อรหัสผ่านที่คอมพิวเตอร์สร้างให้จะยากต่อการจดจำ แตกต่างกัน ผู้ตอบแบบสอบถามเพศชายเห็นด้วยมากกว่าว่าหากคอมพิวเตอร์สร้างรหัสผ่านให้ทั้งหมดจะยากต่อการจดจำมากกว่าผู้ตอบแบบสอบถามเพศหญิง

(3) อายุและรูปภาพที่จะนำมาใช้สร้างรหัสผ่านประเภทภาพบุคคลที่มีชื่อเสียง มีความสัมพันธ์กันอย่างมีนัยสำคัญทางสถิติ ผลการวิเคราะห์ (Person Chi-Square มีค่าเท่ากับ 27.438 df = 16 Sig = .037) ชี้ให้เห็นว่าอายุที่แตกต่างกัน มีความคิดเห็นต่อรูปภาพที่จะนำมาใช้สร้างรหัสผ่านประเภทภาพบุคคลที่มีชื่อเสียง แตกต่างกัน ผู้ตอบแบบสอบถามอายุ 21-30 ปี เห็นด้วยมากกว่าว่าควรนำรูปภาพบุคคลที่มีชื่อเสียงมาใช้ในการสร้างรหัสผ่านมากกว่าผู้ตอบแบบสอบถามทุกช่วงอายุ

(4) ระดับการศึกษาและรหัสผ่านที่คอมพิวเตอร์สร้างให้จะยากต่อการจดจำ มีความสัมพันธ์กันอย่างมีนัยสำคัญทางสถิติ ผลการวิเคราะห์ (Person Chi-Square มีค่าเท่ากับ 26.179 df = 8 Sig = .001) ชี้ให้เห็นว่าระดับการศึกษามีความคิดเห็นต่อรหัสผ่านที่คอมพิวเตอร์สร้างให้จะยากต่อการจดจำ แตกต่างกัน ผู้ตอบแบบสอบถามระดับปริญญาตรีและสูงกว่าปริญญาตรี เห็นด้วยมากกว่าว่าหากคอมพิวเตอร์สร้างรหัสผ่านให้ทั้งหมดจะยากต่อการจดจำมากกว่าผู้ตอบแบบสอบถาม

(5) อาชีพและรหัสผ่านที่คอมพิวเตอร์สร้างให้จะช่วยเป็นแนวทางในการสร้างรหัสผ่าน มีความสัมพันธ์กันอย่างมีนัยสำคัญทางสถิติ ผลการวิเคราะห์ (Person Chi-Square มีค่าเท่ากับ 26.179 df = 8 Sig = .001) ชี้ให้เห็นว่าอาชีพมีความคิดเห็นต่อรหัสผ่านที่คอมพิวเตอร์สร้างให้จะช่วยเป็นแนวทางในการสร้างรหัสผ่าน แตกต่างกัน ผู้ตอบแบบสอบถามอาชีพพนักงานบริษัทเอกชนและนักเรียน/นักศึกษา เห็นด้วยมากกว่าว่าหากคอมพิวเตอร์สร้างรหัสผ่านให้ทั้งหมดจะช่วยเป็นแนวทางในการสร้างรหัสผ่าน มากกว่าผู้ตอบแบบสอบถามอาชีพอื่น

(6) อาชีพและรูปภาพที่จะนำมาใช้สร้างรหัสผ่านประเภทภาพสิ่งมีชีวิต มีความสัมพันธ์กันอย่างมีนัยสำคัญทางสถิติ ผลการวิเคราะห์ (Person Chi-Square มีค่าเท่ากับ 26.510 df = 16 Sig = .047) ชี้ให้เห็นว่าอาชีพที่แตกต่างกัน มีความคิดเห็นต่อรูปภาพที่จะนำมาใช้สร้างรหัสผ่านประเภทภาพสิ่งมีชีวิต แตกต่างกัน ผู้ตอบแบบสอบถามอาชีพพนักงานบริษัทเอกชนและนักเรียน/นักศึกษา เห็นด้วยมากกว่าว่าควรนำรูปภาพประเภทภาพสิ่งมีชีวิต มาใช้ในการสร้างรหัสผ่านมากกว่าผู้ตอบแบบสอบถามอาชีพอื่น

ไม่พบความสัมพันธ์อื่นระหว่างข้อมูลส่วนตัวของผู้ตอบแบบสอบถามกับปัจจัยที่มีต่อการสร้างรหัสผ่านรูปภาพ นอกจากนี้ยังมีคำถามอื่นอีกมากมายที่ไม่สามารถทำการสำรวจได้ เนื่องจากรูปแบบของปัจจัยที่นำมาสำรวจที่ไม่สามารถทำการสำรวจได้ในทุกกรณี

การสำรวจครั้งนี้ใช้วิธีการโพสต์แบบสอบถามออนไลน์ จึงไม่สามารถควบคุมกลุ่มผู้ตอบแบบสอบถามได้ อาจทำให้ผลการวิเคราะห์เพิ่มเติมเกิดความคลาดเคลื่อน ซึ่งหากต้องการนำปัจจัยดังกล่าวไปใช้จริง ต้องมีการนำผลที่ได้

จากการสำรวจทบทวนเพื่อสำรวจกับกลุ่มอื่นต่อไป นอกจากนั้นการใช้วิธีการที่เป็นการสำรวจแบบสอบถามออนไลน์ ก็เป็นลักษณะการสำรวจที่จะได้ข้อมูลออกมาอีกลักษณะหนึ่ง ซึ่งเป็นวิธีการสำรวจที่ระเบียบวิธีวิจัยได้เริ่มใช้กันมากขึ้น เข้าถึงกลุ่มของผู้ใช้หรือกลุ่มตัวอย่างอีกวิธีหนึ่ง และวิธีการสำรวจด้วยวิธีแบบสอบถามออนไลน์ ก็น่าจะเป็นวิธีที่เหมาะสมกับการทำวิจัยของเราที่น่าจะเข้าถึงกลุ่มเป้าหมายของผู้ใช้อินเทอร์เน็ตและต้องใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) มากกว่าการสำรวจด้วยตนเองแบบสัมภาษณ์หรือทางไปรษณีย์

4. สรุปผล

งานวิจัยชิ้นนี้เป็นการวิจัยเชิงสำรวจถึงปัจจัยในการออกแบบรหัสผ่านรูปภาพแบบกริด และจากการเก็บข้อมูลโดยใช้แบบสอบถามออนไลน์กับกลุ่มตัวอย่างที่เป็นผู้ตอบแบบสอบถามจำนวน 423 คน พบว่า ผู้ตอบแบบสอบถามเห็นควรที่ใช้ตารางกริดขนาด 4*4 ที่เป็นรูปแบบจัตุรัส และรูปภาพที่ควรนำมาสร้างเป็นรหัสผ่านควรเป็นรูปภาพแบบรูปธรรม ซึ่งควรเป็นรูปภาพสิ่งมีชีวิตและรูปภาพเหมือนจริง ซึ่งจะเห็นได้ว่าสอดคล้องกับงานวิจัยที่ผ่านมาในแง่ของการนำรูปภาพที่เป็นรูปธรรมมาใช้ในการสร้างรหัสผ่านรูปภาพ (Graphical Password) จำนวนไอคอนรูปภาพที่จะใช้เป็นตัวเลือกสร้างรหัสผ่านรูปภาพควรมีจำนวน 30 รูปภาพและรูปแบบการได้มาของรหัสผ่านที่มีคะแนนเฉลี่ยที่ใกล้เคียงกันมากระหว่างคอมพิวเตอร์สร้างให้บางส่วนและผู้ใช้งานสร้างเพิ่มเองบางส่วนกับผู้ใช้งานสร้างรหัสผ่านเองทั้งหมดจึงเป็นประเด็นที่น่าสนใจที่จะนำมาทำการวิจัยเชิงทดลอง ซึ่งน่าจะทำให้ได้รหัสผ่านที่ดีเพราะสอดคล้องกับงานวิจัยที่ผ่านมาเกี่ยวกับการสร้างรหัสผ่านแบบตัวอักษร (Text Password) และปัจจัยสำคัญสุดท้ายในการสำรวจครั้งนี้คือ รูปแบบของปฏิสัมพันธ์ในการสร้างรหัสผ่านรูปภาพควรเป็นแบบ Point and Click โดยรหัสผ่านรูปภาพสามารถมีรูปภาพที่ซ้ำกันได้ เพื่อความหลากหลายของรหัสผ่านรูปภาพมากขึ้น

5. ข้อเสนอแนะ

จากการสำรวจครั้งนี้สามารถนำผลที่ได้จากการสำรวจทำการศึกษาเพิ่มเติม ไม่ว่าจะเป็นพฤติกรรมในการสร้างรหัสผ่าน รูปแบบการป้องกันการโจรกรรม ขนาด (กว้าง* ยาว) ของรูปภาพหรือจำนวนภาพที่เหมาะสมสำหรับใช้เป็นมาตรฐานในการสร้างรหัสผ่าน โดยดูจากความจำของมนุษย์ว่าสามารถที่จำรูปภาพได้จำนวนเท่าไร จึงจะเหมาะสมเมื่อเปรียบเทียบกับการสร้างรหัสผ่านที่เป็นตัวอักษร และนำผลที่ได้จากการสำรวจปัจจัยครั้งนี้พัฒนาและออกแบบการวิจัยเชิงการทดลองเกี่ยวกับรหัสผ่านรูปภาพแบบกริด ที่มีการทดสอบความสมดุลย์ระหว่างระดับความปลอดภัยกับความง่ายในการจดจำและความสะดวกในการใช้ของผู้ใช้ต่อไป

6. กิตติกรรมประกาศ

ขอขอบพระคุณผู้ตอบแบบสอบถามทุกท่านอย่างสูงที่กรุณาสละเวลาในการเข้ามาตอบแบบสำรวจในครั้งนี้

7. เอกสารอ้างอิง

[1] RealUser. Retrieved 1 august 2013, from www.realuser.com

[2] Sobrado, L., & Birget, J. C. (2002). Graphical passwords. The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, Vol. 9.

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

[4] Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The Design and Analysis of Graphical Passwords. In Proceedings of the 8th USENIX Security Symposium.

[5] Farnaz, T., Maslin, M., & Azizah A. M. (2013). S-Passface: An Enhancement on Passface Graphical Password Authentication. Journal of Basic and Applied Scientific Research

[6] Takada, T., & Koike, H. (2003). Awase-E: Image-based authentication for mobile phones using user's favorite images. Human-Computer Interaction with Mobile Devices and Services, vol. 2795, 347-351.

[7] Thorpe, J., & van Oorschot, P. C. (2004). Towards secure design choices for implementing graphical passwords. 20th Annual Computer Security Applications Conference (ACSAC).

[8] Majid, A.,Douglas, S., & Behzad, M. (2013). Usability and Security of Gaze-Based Graphical Grid Passwords. Lecture Notes in Computer Science (Financial Cryptography and Data Security: FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers), Springer, Okinawa, Japan, pp. 17-33.

[9] Fleming, M. L. & Sheikhian, M. (1972). Influence of pictorial attributes on recognition memory. AV Communication Review, 20, 423-441.

[10] Shepard, R. N. (1967). Recognition memory for words, sentences, and pictures. Journal of Verbal Learning and Verbal Behavior, Vol. 6, pp. 156-163.

[11] Tao, H., & Adams, C. (2006). Pass-Go: A proposal to improve the usability of graphical passwords. International Journal of Network Security, Vol. 7(2), 273-292.