การวิเคราะห์ความแข็งแรงของนโยบายรหัสผ่านของเว็บไซต์ในประเทศไทย และแนวทางแนะนำสำหรับเว็บไซต์แต่ละประเภท

AN ANALYSIS OF PASSWORD COMPOSITION POLICY STRENGTH OF WEBSITES IN THAILAND AND THE RECOMMENDED GUIDELINE FOR EACH WEBSITE CATEGORY

เจนจิรา ล้อมจันทร์

JENJIRA LOMCHAN

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร
ปริญญาวิทยาศาสตรมหาบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์
ภาควิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ. 2566

KMITL-2023-SC-M-002-049

AN ANALYSIS OF PASSWORD COMPOSITION POLICY STRENGTH OF WEBSITES IN THAILAND AND THE RECOMMENDED GUIDELINE FOR EACH WEBSITE CATEGORY

JENJIRA LOMCHAN

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE

DEPARTMENT OF COMPUTER SCIENCE SCHOOL OF SCIENCE
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG

2023

KMITL-2023-SC-M-002-049

หัวข้อวิทยานิพนธ์	การวิเคราะห์ความแข็งแรงของนโยบายรหัสผ่านของเว็บไซต์ในประเทศไทย และแนวทางแนะนำสำหรับเว็บไซต์แต่ละประเภท
นักศึกษา	นางสาวเจนจิรา ล้อมจันทร์
รหัสประจำตัว	60605073
ปริญญา	วิทยาศาสตรมหาบัณฑิต (วิทยาการคอมพิวเตอร์)
ภาควิชา	วิทยาการคอมพิวเตอร์
พ.ศ.	2566
อาจารย์ที่ปรึกษาวิทยานิพนธ์	ดร. รุ่งรัตน์ เวียงศรีพนาวัลย์

บทคัดย่อ

งานวิจัยนี้ประกอบไปด้วยสองส่วน ส่วนที่หนึ่งคือการศึกษาและเปรียบเทียบความแข็งแรงของนโยบายรหัสผ่านของเว็บไซต์ในประเทศไทยกับเว็บไซต์ในประเทศสหรัฐอเมริกาและประเทศเยอรมนีที่ศึกษาโดย D. Florêncio, C. Herley, P. C. Van Oorschot, P. Mayer, J. Kirchner และ M. Volkamer ผลการวิจัยพบว่าในขณะที่เว็บไซต์หน่วยงานของรัฐในประเทศสหรัฐอเมริกาและประเทศเยอรมันมีความแข็งแรงของนโยบายรหัสผ่านที่สูงกว่าเว็บไซต์ประเภทธนาคารและมหาวิทยาลัยหน่วยงานรัฐไทยค่านี้ในภาพรวมต่ำที่สุดถึงแม้ว่าหลังจากการประกาศใช้พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลหน่วยงานของรัฐบางหน่วยงานมีการเพิ่มความแข็งแรงของนโยบายรหัสผ่านของเว็บไซต์ที่เพิ่มขึ้น ในงานวิจัยในส่วนที่สองจึงมีการสำรวจเว็บไซต์หน่วยงานของรัฐ เว็บไซต์ที่ให้บริการซื้อขายสินค้า และเว็บไซต์ผู้ให้บริการด้านโรงแรมและการเดินทางในประเทศไทยว่ามีการปฏิบัติตามมาตรฐานสากลในการตั้งรหัสผ่านหรือไม่ เนื่องจากหนึ่งในสมมติฐานเรื่องนโยบายรหัสผ่านที่ไม่แข็งแรงคือการขาดความตระหนักรู้ของผู้พัฒนาเว็บแอปพลิเคชันในเรื่องมาตรฐานสากลของนโยบายรหัสผ่าน ผลการวิจัยพบว่ามีเว็บไซต์เพียง 22 เว็บไซต์จากกลุ่มตัวอย่างทั้งหมด 40 เว็บไซต์ที่มีนโยบายการกำหนดรหัสผ่านในด้านความยาวและความซับซ้อนที่ตรงตามมาตรฐานแต่นโยบายอื่นเช่น ห้ามใช้รหัสผ่านที่เดาง่าย ไม่มีเว็บไซต์ใดมีการตั้งนโยบายในข้อนี้แม้จะมียอดผู้ใช้งานค่อนข้างสูง ดังนั้นงานวิจัยนี้จึงมีวัตถุประสงค์หลักในการนำเสนอแนวทางในการกำหนดตนโยบายรหัสผ่านเว็บไซต์เพื่อให้มีความแข็งแรงและปลอดภัยตามมาตรฐานที่บังคับใช้ในหน่วยงานรัฐไทย เช่น สกมช. และตามมาตรฐานสากล เช่น เอ็นไอเอสทีและพีซีไอดีเอสเอส ให้กับผู้พัฒนาเว็บไซต์โดยจะมีการจำแนกนโยบายจากข้อมูลที่ทางเว็บไซต์เข้าถึงหรือเก็บ ทั้งนี้แนวทางการกำหนดนโยบายรหัสผ่านดังกล่าวได้รับความเห็นชอบจากผู้เชี่ยวชาญ สำหรับในส่วนของผู้ใช้งานนั้น

งานวิจัยนี้มีการสำรวจความเต็มใจที่จะปฏิบัติตามนโยบายของผู้ใช้บริการในนโยบายแต่ละข้อ ผลการสำรวจพบว่าผู้ใช้บริการชาวไทยเพื่อประโยชน์ในเรื่องความปลอดภัยแม้จะไม่เต็มใจแต่พร้อมที่จะปฏิบัติตาม

Thesis	An analysis of Password Composition Policy strength of websites in Thailand and the recommended guideline for each website category
Student	Miss. Jenjira Lomchan
Student ID	60605073
Degree	Master of Science (Computer Science)
Department	Computer Science
Year	2023
Thesis Advisor	Dr. Rungrat Wiangsripanawan

ABSTRACT

This research consists of two parts. The first part is a study and comparison of the password composition policy (PCP) strength of Thai websites with those in the United States and Germany. The results showed that while government agency sites in the United States and Germany had higher password policy strength than those of banking and university sites, this value was the lowest for Thai government agency sites. Although after the announcement of the Thai Personal Data Protection Act, some government agencies had increased the strength of website password policies. In the second part of the research, since one of the assumptions about unhealthy PCP is the lack of awareness among web application developers, a survey whether government agency websites, trading websites and hotel and travel service websites in Thailand followed national/international standards for PCPs or not was conducted. The research found that only 22 websites out of a total sample of 40 websites had policies for requiring passwords in terms of length and complexity that met the standards. No website has a policy on "do not use passwords that are easy to guess", despite the relatively high number of users. Hence, this research main objective is to present a guideline for establishing website PCPs to be strong and secure in accordance with the standards enforced in Thai government agencies such as NCSA and international standards, such as NIST and PCIDSS. Guideline policies will be distinguished from the information that the websites access or

collect and have been approved by experts. As for users, this research explored users' willingness to comply with each policy. The survey found that Thai users for the sake of safety, although unwilling, ready to comply.

กิตติกรรมประกาศ

ขอขอบคุณ อ.ดร. รุ่งรัตน์ เวียงศรีพนาวัลย์ ที่ให้ความอนุเคราะห์รับเป็นอาจารย์ที่ปรึกษา และให้คำแนะนำ คำปรึกษามาโดยตลอด รวมถึงช่วยตรวจสอบปริญญานิพนธ์นี้ ให้มีความถูกต้องครบถ้วนสมบูรณ์ และคณะกรรมการสอบวิทยานิพนธ์ทุกท่าน

ขอขอบคุณ PhD. Siamak F. Shahandashti ที่ให้คำแนะนำ ให้คำปรึกษาในการค้นคว้าวิจัย ผลงานที่ได้รับการตีพิมพ์อย่างดีเสมอมา

ขอขอบคุณเพื่อน พี่ น้อง ชมรมอาสาพัฒนาพระจอมเกล้าเจ้าคุณทหารลาดกระบัง บ้านใบไม้ สมาคมชาวเดินป่า สมาคมชาวบาร์น้ำวน หัวหน้างานและเพื่อนร่วมงาน ที่ช่วยให้ข้อมูล และร่วมตอบแบบสอบถามในงานวิจัยนี้

ขอขอบคุณเพื่อนร่วมรุ่น หลักสูตรปริญญาโทวิทยาการคอมพิวเตอร์ สจล. รุ่นรหัส 60 ที่ช่วยเหลือ ให้คำแนะนำ ให้กำลังใจกันในการเรียนหลักสูตรนี้เสมอมา

เจนจิรา ล้อมจันทร์

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูป

รูปที่ **หน้า**

คำย่อ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	ศปช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	สกมช
Business to Customer	B2C
Multi Factor Authentication	MFA
National Institute of Standards and Technology	NIST
Open Worldwide Application Security Project	OWASP
Password Composition Policy	PCP
Payment Card Industry Data Security Standard	PCI DSS
Two Factor Authentication	2FA

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของงานวิจัย

เนื่องมาจากงานวิจัยเรื่อง The Comparison of Password Composition Policies among US, German, and Thailand Samples [9] ผู้วิจัยได้ทำการศึกษาและเปรียบเทียบปัจจัยที่มีผลต่อนโยบายการกำหนดรหัสผ่านของเว็บไซต์แต่ละประเภทในประเทศสหรัฐอเมริกา ประเทศเยอรมนี และประเทศไทย ซึ่งปัจจัยที่ใช้ในการศึกษาเว็บไซต์ในประเทศสหรัฐอเมริกาและเยอรมันมีทั้งหมด 6 ปัจจัย คือ ขนาดของบริการ, มูลค่าสินทรัพย์, เว็บไซต์รองรับโฆษณา, เว็บไซต์มีการโฆษณาบนเว็บไซต์อื่น, ผู้ใช้สามารถเลือกที่จะใช้หรือไม่ใช้งาน และเว็บไซต์เคยถูกพบปัญหา data breach และเนื่องจากช่วงเวลาที่ผ่านมาเทคโนโลยีที่เกี่ยวข้องได้ถูกพัฒนาและบังคับใช้มากขึ้น เช่น google บังคับใช้ HTTPS, การใช้ Two-Factor Authentication เพื่อเพิ่มความปลอดภัยให้บัญชีผู้ใช้งาน ผู้วิจัยจึงศึกษาเพิ่มอีก 2 ปัจจัยที่คาดว่าจะมีผลกับนโยบายความปลอดภัยของรหัสผ่าน คือ HTTPS และ 2FA นอกจากนี้ในปี 2019 ประเทศไทยประกาศกฎหมายคุ้มครองข้อมูลส่วนบุคคล จึงได้มีการศึกษาเปรียบเทียบกลุ่มตัวอย่างเว็บไซต์ในประเทศไทยหลังประกาศใช้กฎหมายดังกล่าว ผลการศึกษาพบว่าปัจจัยที่มีผลกับนโยบายการกำหนดรหัสผ่านของเว็บไซต์ในประเทศไทย ตรงข้ามกับประเทศสหรัฐอเมริกาและประเทศเยอรมนี โดยสรุปคือปัจจัยที่มีผลด้านความปลอดภัย เช่น มูลค่าของสินทรัพย์ที่ไม่มีผลต่อนโยบายการกำหนดรหัสผ่านเว็บไซต์ของประเทศสหรัฐอเมริกาและประเทศเยอรมนี แต่กลับมีผลกับเว็บไซต์ของประเทศไทย บางเว็บไซต์ในประเทศเยอรมณีที่ใช้ 2FA อนุญาตให้ใช้ PCP ที่ต่ำกว่าเพื่อการใช้งานที่ดีขึ้น แต่เว็บไซต์ในประเทศไทยที่มี 2FA ก็ไม่ได้คลายข้อกำหนดรหัสผ่าน เว็บไซต์หน่วยงานรัฐไทยมีนโยบายการกำหนดรหัสผ่านที่ต่ำกว่าประเทศสหรัฐอเมริกาและประเทศเยอรมนี แม้จะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลบังคับใช้ในประเทศไทย[19] หลังประกาศใช้กฎหมายดังกล่าวพบเพียง 2 จาก 10 หน่วยงานรัฐที่ปรับนโยบายการกำหนดรหัสผ่านให้มีความปลอดภัยมากขึ้น ถึงแม้ว่าเว็บไซต์เหล่านั้นมีการเก็บข้อมูลส่วนบุคคลของผู้ใช้งานก็ตาม

เนื่องจากการใช้งานเว็บไซต์ส่วนใหญ่จำเป็นต้องระบุชื่อผู้ใช้และรหัสผ่านในการเข้าสู่ระบบ ซึ่งมีข้อตกลงและนโยบายในการกำหนดรหัสผ่านมีความแตกต่างกัน บางระบบตระหนักถึงความปลอดภัยจึงมีการใช้นโยบายการกำหนดรหัสผ่านที่แข็งแรง รวมถึงอาจใช้ 2FA ร่วมด้วย ในขณะเดียวกัน บางระบบลดความปลอดภัยลงด้วยการใช้นโยบายการกำหนดรหัสผ่านที่ต่ำ เพื่อสร้างความสะดวกแก่ผู้ใช้งาน ซึ่งในปัจจุบันประเทศไทยยังไม่มีการกำหนดนโยบายในการกำหนดรหัสผ่านของเว็บไซต์แต่ละประเภทที่ชัดเจน ผู้พัฒนาทำการกำหนดและปรับใช้ตามแต่ละองค์กร ซึ่งอาจไม่มีความเข้าใจเพียงพอ ทำให้เรามัก

ได้ยินข่าวข้อมูลรั่วไหลจากเว็บไซต์ขององค์กรต่างๆ อยู่เป็นระยะ และน่าแปลกใจที่ข่าวข้อมูลรั่วไหลในประเทศไทย ส่วนใหญ่เป็นเว็บไซต์หน่วยงานรัฐ ซึ่งอาจเกิดจากช่องโหว่ที่ยินยอมให้ผู้ใช้กำหนดรหัสผ่านที่ไม่ปลอดภัย และใช้รหัสผ่านเพียงอย่างเดียวในการเข้าสู่ระบบ เมื่อผู้ให้พัฒนาและผู้ใช้บริการไม่ได้ตระหนักถึงความปลอดภัยจากข้อตกลงและนโยบายการกำหนดรหัสผ่านที่ไม่แข็งแรง จึงส่งผลให้ข้อมูลของผู้ใช้บริการถูกเข้าถึงอย่างไม่พึงประสงค์ และผู้ไม่หวังดีนำข้อมูลดังกล่าวไปใช้อย่างผิดกฎหมาย นอกจากนี้ผู้ให้บริการเว็บไซต์ยังเสียความน่าเชื่อถือต่อผู้ใช้บริการ ปัจจุบันโลกของเราอยู่ในยุคดิจิทัลที่ข้อมูลต่างๆ อยู่ในรูปแบบออนไลน์ เป็นฐานข้อมูลขนาดใหญ่ที่สามารถถูกนำไปใช้ประโยชน์ได้ทั้งในด้านดีและไม่ดี ดังนั้นเพื่อเป็นการป้องกันความเสี่ยงข้อมูลรั่วไหล ผู้ให้บริการเว็บไซต์โดยเฉพาะหน่วยงานรัฐที่มีข้อมูลของประชาชนอยู่ในระบบ รวมถึงเว็บไซต์ที่มีผู้ใช้บริการเป็นจำนวนมากควรสร้างข้อตกลงและนโยบายในการกำหนดรหัสผ่านที่แข็งแรงและเป็นไปตามมาตรฐานสากล

ในช่วง 2-3 ปีที่ผ่านมาประชาชนต้องใช้ชีวิตเปลี่ยนไปจากเดิมเนื่องจากโรคระบาดโควิด-19 ก่อนเกิดโรคระบาดประชาชนเดินทางไปซื้อสินค้าที่ใช้ในชีวิตประจำวันที่ร้านค้า ห้างสรรพสินค้า ตลาดด้วยตนเอง แต่เพื่อลดความเสี่ยงการติดเชื้อจากโรคระบาด จึงเริ่มอาศัยเว็บไซต์อีคอมเมิร์ซในการซื้อสินค้าที่ต้องใช้ในชีวิตประจำวันมากขึ้น ซึ่งการซื้อสินค้าออนไลน์จำเป็นต้องระบุข้อมูลส่วนตัว เช่น ชื่อ-นามสกุล ที่อยู่ปัจจุบันสำหรับจัดส่งสินค้า หมายเลขโทรศัพท์มือถือ เป็นต้น นอกจากนี้เพื่ออำนวยความสะดวกต่อผู้ใช้บริการบางเว็บไซต์เพิ่มตัวเลือกการชำระเงินแบบตัดผ่านบัตรเครดิต และสามารถเก็บบันทึกข้อมูลบัตรเครดิตเพื่อใช้ซื้อสินค้าในเว็บไซต์ครั้งถัดไปได้โดยไม่ต้องกรอกข้อมูลใหม่ ซึ่งถือว่าอันตรายเป็นอย่างมากหากข้อมูลดังกล่าวรั่วไหล และเมื่อเริ่มมีการผ่อนปรนมาตรควบคุมการสถานการณ์โควิด-19 ประชาชนเริ่มเดินทางท่องเที่ยวมากขึ้น อีกหนึ่งอุตสาหกรรมที่กลับมาเติบโตหลังผ่อนปรนมาตรการควบคุมโรคระบาดคือเว็บไซต์ที่ให้บริการด้านโรงแรมและการเดินทาง และเช่นเดียวกันเว็บไซต์เหล่านี้มีการเก็บข้อมูลส่วนบุคคลและข้อมูลการชำระเงินเช่นเดียวกับเว็บไซต์ที่ให้บริการซื้อขายสินค้า

จากผลงานวิจัยและข้อมูลข้างต้น ผู้วิจัยจึงต้องการวิเคราะห์ความปลอดภัยและเปรียบเทียบนโยบายในการกำหนดรหัสผ่านบนเว็บไซต์หน่วยงานรัฐ เว็บไซต์ที่ให้บริการซื้อขายสินค้า และเว็บไซต์ผู้ให้บริการด้านโรงแรมและการเดินทางในประเทศไทย และเสนอแนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์แต่ละประเภทให้เป็นไปตามมาตรฐานสากล รวมถึงพัฒนาเครื่องมือที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่าน โดยที่นโยบายดังกล่าวมีความปลอดภัยเพิ่มขึ้นแต่ไม่สร้างความยากลำบากต่อผู้ใช้บริการ

1.2 วัตถุประสงค์ของงานวิจัย

1) เพื่อวิเคราะห์ความปลอดภัยและเปรียบเทียบนโยบายในการกำหนดรหัสผ่านบนเว็บไซต์หน่วยงานรัฐบาล เว็บไซต์ที่ให้บริการซื้อขายสินค้า และเว็บไซต์ด้านโรงแรมและการเดินทางในประเทศไทย ว่าเป็นไปตามมาตรฐานหรือไม่
2) เพื่อเสนอแนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์แต่ละประเภทให้เป็นไปตามมาตรฐานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, NIST และ PCI DSS
3) เพื่อพัฒนาแนวปฏิบัติที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่านสำหรับผู้พัฒนาระบบ
4) เพื่อสำรวจระดับความยากง่ายและความเต็มใจของผู้ใช้บริการในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านตามมาตรฐานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, NIST และ PCI DSS

1.3 ขอบเขตของงานวิจัย

1) งานวิจัยนี้ครอบคลุมเว็บไซต์หน่วยงานรัฐไทยจากสำนักงานสถิติแห่งชาติที่มีระบบล็อกอินสำหรับประชาชนทั่วไป และมีการเก็บข้อมูลส่วนบุคคลเท่านั้น
2) งานวิจัยนี้ครอบคลุมเว็บไซต์ที่ให้บริการซื้อขายสินค้า เว็บไซต์ด้านโรงแรมและการเดินทางในประเทศไทยที่มีผู้เข้าชมสูงสุด 10 อันดับแรกเท่านั้น
3) งานวิจัยนี้ครอบคลุมการศึกษาข้อตกลงและนโยบายในการกำหนดรหัสผ่านเว็บไซต์โดยอ้างอิงจากมาตรฐานสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, NIST และ PCI DSS เท่านั้น

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1) สามารถวิเคราะห์ความปลอดภัยเปรียบเทียบนโยบายในการกำหนดรหัสผ่านบนเว็บไซต์หน่วยงานรัฐบาล เว็บไซต์ที่ให้บริการซื้อขายสินค้า และเว็บไซต์ด้านโรงแรมและการเดินทางในประเทศไทย ว่าเป็นไปตามมาตรฐานหรือไม่
2) สามารถเสนอแนวทางการกำหนดรหัสผ่านตามมาตรฐานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ, NIST และ PCI DSS เพื่อปรับใช้กับเว็บไซต์แต่ละประเภทได้อย่างเหมาะสม
3) สามารถพัฒนาแนวปฏิบัติที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่านสำหรับผู้พัฒนาระบบได้
4) สามารถนำนโยบายการกำหนดรหัสไปปรับใช้กับเว็บไซต์แต่ละประเภทได้อย่างเหมาะสม และผู้ใช้บริการสามารถปฏิบัติตามได้

บทที่ 2
ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

บทนี้จะกล่าวถึงทฤษฎีและข้อมูลที่เกี่ยวข้องกับงานวิจัย อันประกอบด้วย งานวิจัยที่เกี่ยวข้องในหัวข้อเรื่อง The Comparison of Password Composition Policies among US, German, and Thailand Samples, การคำนวณค่า PCP Strength, การตรวจสอบเว็บไซต์ยินยอมให้กำหนดรหัสผ่านที่ไม่ปลอดภัย, การตรวจสอบเว็บไซต์ที่ถูกพบ Data Breach, ข้อมูลส่วนบุคคล, นโยบายในการกำหนดรหัสผ่านตามมาตรฐานของ NIST, นโยบายในการกำหนดรหัสผ่านตามมาตรฐานของ PCI DSS, สถิติการเข้าใช้บริการเว็บไซต์ในประเทศไทย, ช่องทางการชำระเงินผ่านเว็บไซต์ในประเทศไทย และการประเมินความเต็มใจในการใช้บริการ

2.1 งานวิจัยที่เกี่ยวข้อง

จากงานวิจัยเรื่อง The Comparison of Password Composition Policies among US, German, and Thailand Samples [8] ผู้วิจัยได้ทำการศึกษาและเปรียบเทียบปัจจัยที่มีผลต่อนโยบายการกำหนดรหัสผ่านของเว็บไซต์แต่ละประเภทในประเทศสหรัฐอเมริกาปี 2010, ประเทศสหรัฐอเมริกาปี 2016, ประเทศเยอรมนีปี 2016, ประเทศไทยปี 2018 และประเทศไทยปี 2021 โดย Password Composition Policies (PCPs) หมายถึงนโยบายการกำหนดรหัสผ่านเว็บไซต์ที่กำหนดให้ต้องระบุรหัสผ่านที่มีความยาวขั้นต่ำเท่าใดและต้องประกอบด้วยตัวอักษรประเภทใดบ้าง และต้องการศึกษาว่าปัจจัยใดบ้างที่คาดว่ามีผลกับนโยบายการกำหนดรหัสผ่าน โดยงานวิจัยดังกล่าวได้ศึกษาเปรียบเทียบกับงานวิจัยตั้งต้น 6 ปัจจัย คือ

1. ขนาดของบริการ
2. มูลค่าสินทรัพย์
3. เว็บไซต์รองรับโฆษณา
4. เว็บไซต์มีการโฆษณาบนเว็บไซต์อื่น
5. ผู้ใช้สามารถเลือกที่จะใช้หรือไม่ใช้งาน
6. เว็บไซต์เคยถูกพบปัญหา data breach

และศึกษาเพิ่มเติมอีก 2 ปัจจัยที่คาดว่าจะมีผลกับนโยบายการกำหนดรหัสผ่าน คือ HTTPS และ Two-Factor Authentication (2FA)

ผลการวิจัยพบว่าปัจจัยที่มีผลต่อนโยบายการกำหนดรหัสผ่านของเว็บไซต์กลุ่มตัวอย่างในประเทศไทยคือ มูลค่าสินทรัพย์ เว็บไซต์รองรับโฆษณา ผู้ใช้สามารถเลือกที่จะใช้หรือไม่ใช้งาน และ 2FA ผลของค่าความแข็งแกร่งของนโยบายการกำหนดรหัสผ่าน (PCP Strength) โดยรวมของกลุ่มตัวอย่างไทยและเยอรมันเท่ากันและต่ำกว่าตัวอย่างในสหรัฐอเมริกา เว็บไซต์ธนาคารในประเทศไทยมีค่า PCP Strength สูงสุด แต่เว็บไซต์ของรัฐบาลให้ค่า PCP Strength ต่ำที่สุดจากตัวอย่างทั้งหมด ดังแสดงในตารางที่ 2.1

ตารางที่ 2.1 ค่ามัธยฐานของค่าความแข็งแกร่งของนโยบายการกำหนดรหัสผ่านในแต่ละกลุ่มเว็บไซต์

The median of PCP strength								
Sample	Overall	Traffic rank				Bank	Uni.	Gov.
		Top	High	Med	Low			
USA 2010	35.7	19.9	19.9	36.2	19.9	31.0	41.7	47.6
USA 2016	41.4	26.6	41.5	46.5	29.9	35.7	47.6	52.7
GER 2016	26.6	26.6	25.8	19.9	26.6	16.6	30.8	47.6
THA 2018	26.6	19.9	26.6	16.6	13.3	41.4	41.4	29.9
THA 2021	31.0	26.6	26.6	18.3	19.9	41.4	47.5	40.4

จากตารางที่ 2.1 แสดงให้เห็นถึงความแตกต่างของค่าความแข็งแกร่งของนโยบายการกำหนดรหัสผ่านในแต่ละกลุ่มเว็บไซต์ เมื่อเปรียบเทียบระหว่างประเทศสหรัฐอเมริกา เยอรมณี และประเทศไทย พบว่าประเทศไทยในปี 2018 และประเทศเยอรมณีในปี 2016 มีค่า PCP Strength เท่ากันคือ 26.6 แต่ยังคงต่ำกว่าประเทศสหรัฐอเมริกา ถึงแม้ว่าในปี 2021 ประเทศไทยมีค่า PCP Strength สูงขึ้นโดยอยู่ที่ 31.0 แต่ยังคงต่ำประเทศสหรัฐอเมริกาเช่นเดิม และเมื่อตรวจสอบในแต่ละประเภทเว็บไซต์พบว่าประเทศไทยมีค่า PCP Strength สูงที่สุดในกลุ่มเว็บไซต์ธนาคารโดยอยู่ที่ 41.4 และมีค่า PCP Strength ต่ำที่สุดในกลุ่มเว็บไซต์หน่วยงานรัฐโดยมีค่าอยู่ที่ 29.9 ในปี 2018 และ 40.4 ในปี 2021

เมื่อเปรียบเทียบค่า PCP Strength ของประเทศไทยในพบว่าค่า PCP Strength สูงขึ้นจากเดิม 26.6 ในปี 2018 สูงขึ้นเป็น 31.0 ในปี 2021 ซึ่งเกิดจาก 12 เว็บไซต์มีการปรับนโยบายการกำหนดรหัสผ่านให้มีความแข็งแกร่งมากขึ้น 2 เว็บไซต์ปรับนโยบายการกำหนดรหัสผ่านให้มีความแข็งแกร่งลดลง และ 61 เว็บไซต์ยังคงกำหนดนโยบายการกำหนดรหัสผ่านตามเดิมแม้มีการประกาศใช้กฎหมายคุ้มครองข้อมูลส่วนบุคคล

ค่า PCP Strength ของเว็บไซต์หน่วยงานรัฐไทยเพิ่มสูงขึ้นในปี 2021 เกิดจากการปรับนโยบายการกำหนดรหัสผ่านจาก 2 เว็บไซต์เท่านั้นคือกรมสรรพากรและสำนักงานสลากกินแบ่งรัฐบาล ในขณะที่อีก 6 เว็บไซต์ยังคงใช้นโยบายการกำหนดรหัสผ่านแบบเดิม

ปัจจัยที่มีผลต่อค่า PCP Strength ของเว็บไซต์ของทุกกลุ่มตัวอย่างมีทั้งเหมือนกันและแตกต่างกันดังแสดงในตารางที่ 2.2

ตารางที่ 2.2 ปัจจัยที่มีผลต่อค่า PCP Strength

Website feature	Actual effect on PCP strength				
	USA 2010	GER 2010	GER 2016	THA 2018	THA 2021
Observation and evidence	-	-	-	-	-
Size of the service	-	-	-	-	-
Value of assets	-	-	-	↑	↑
HTTPS	N/A	N/A	N/A	-	-
2FA	N/A	N/A	N/A	↑	↑
Advertising accepted	↓	↓	-	↓	↓
Site advertises	↓	-	-	-	-
User has choice	↓	↓	↓	↓	↓

จากตารางที่ 2.1 ปัจจัยที่มีผลต่อค่า PCP Strength ในทุกกลุ่มตัวอย่างเว็บไซต์สรุปได้ดังนี้

1. ขนาดของบริการ ไม่มีผลกับ PCP Strength ในทุกกลุ่มตัวอย่าง
2. มูลค่าสินทรัพย์ มีผลกับกลุ่มตัวอย่างเว็บไซต์ในประเทศไทยทั้งในปี 2018 และปี 2021 แต่ไม่มีผลกับกลุ่มตัวอย่างเว็บไซต์ในประเทศสหรัฐอเมริกาและเยอรมนี
3. เว็บไซต์รองรับโฆษณา ไม่มีผลกับกลุ่มตัวอย่างเว็บไซต์ในประเทศเยอรมนีปี 2016 แต่มีผลกับกลุ่มตัวอย่างเว็บไซต์อื่น

4. เว็บไซต์มีการโฆษณาบนเว็บไซต์อื่น มีผลกับกลุ่มตัวอย่างเว็บไซต์ในประเทศสหรัฐอเมริกาปี 2010 แต่ไม่มีผลกับกลุ่มตัวอย่างเว็บไซต์อื่น
5. ผู้ใช้สามารถเลือกที่จะใช้หรือไม่ใช้งาน มีผลกับ PCP Strength ในทุกกลุ่มตัวอย่าง
6. เว็บไซต์เคยถูกพบปัญหา data breach ไม่มีผลกับ PCP Strength ในทุกกลุ่มตัวอย่าง
7. HTTPS ไม่มีผลกับ PCP Strength กลุ่มตัวอย่างเว็บไซต์ในประเทศไทยทั้งในปี 2018 และปี 2021
8. Two-Factor Authentication มีผลกับ PCP Strength กลุ่มตัวอย่างเว็บไซต์ในประเทศไทยทั้งในปี 2018 และปี 2021

2.2 การคำนวณค่าความแข็งแกร่งของนโยบายการกำหนดรหัสผ่าน

นโยบายการกำหนดรหัสผ่านเว็บไซต์ในปัจจุบันมีหลากหลายนโยบายตามแต่ผู้พัฒนาเว็บไซต์กำหนด เช่น บางเว็บไซต์บังคับให้รหัสผ่านต้องมีความยาวอย่างน้อย 6 ตัวอักษร บางเว็บไซต์มีข้อบังคับเพิ่มว่ารหัสผ่านต้องประกอบด้วยตัวเลข ตัวอักษร และอักขระพิเศษ เป็นต้น จากนโยบายที่หลากหลายจึงเป็นเรื่องยากที่จะเปรียบเทียบความแข็งแกร่งของนโยบายการกำหนดรหัสผ่าน

การวิจัยนี้ได้ศึกษาการคำนวณค่าความแข็งแกร่งของนโยบายการกำหนดรหัสผ่าน (PCP Strength) [8] ซึ่งถูกใช้อย่างแพร่หลายเพื่อคำนวณหาความแข็งแกร่งของ PCP ที่มีองค์ประกอบคือความยาวขั้นต่ำของรหัสผ่านและอักขระขั้นต่ำที่เว็บไซต์บังคับ และนำผลลัพธ์ที่ได้จากการคำนวณไปใช้เปรียบเทียบ PCP ของแต่ละเว็บไซต์ โดยมีสูตรการคำนวณคือ

$$\text{PCP strength} = N_{min} \times \log_2 C_{min} \quad (1)$$

โดยค่า N หมายถึงความยาวขั้นต่ำของรหัสผ่าน และค่า C หมายถึงจำนวนอักขระขั้นต่ำของรหัสผ่าน ยกตัวอย่างเช่น เว็บไซต์บังคับให้ต้องกำหนดรหัสผ่านอย่างน้อย 6 ตัวอักษร จึงสามารถคำนวณโดยแทนที่ N เท่ากับ 6 และเนื่องจากไม่มีการกำหนดอักขระที่บังคับ ขั้นต่ำของอักขระจึงสามารถระบุตัวเพียงตัวเลขอย่างเดียวได้ ในที่นี้คือ 0 - 9 ดังนั้นจำนวนอักขระที่บังคับจึงเท่ากับ 10 เมื่อแทนที่ C เท่ากับ 10 จะได้ค่า PCP strength เป็น 19.9 bits

ผู้วิจัยได้คำนวณค่า PCP Strength จากนโยบายการกำหนดรหัสผ่านเว็บไซต์ที่พบเจอบ่อย ตัวอย่างเช่น รหัสผ่านต้องมีความยาวอย่างน้อย 6 ตัวอักษร รหัสผ่านต้องมีความยาวอย่างน้อย 6 ตัวอักษรและต้องประกอบด้วยตัวเลขและตัวอักษรภาษาอังกฤษ ดังแสดงในตาราง 2.3

ตารางที่ 2.3 ตัวอย่างค่า PCP Strength

ความยาวรหัสผ่าน	อักขระที่บังคับ	จำนวนอักขระที่บังคับ	ค่า PCP Strength
6	ตัวเลข	10	19.9
7	ตัวเลขและตัวอักษรภาษาอังกฤษ	36	36.2
8	ตัวเลข	10	26.6
8	ตัวเลขและตัวอักษรภาษาอังกฤษ	36	41.4
8	ตัวเลข ตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ และตัวอักษรภาษาอังกฤษพิมพ์เล็ก	62	47.6
8	ตัวเลข ตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ ตัวอักษรภาษาอังกฤษพิมพ์เล็ก และอักขระพิเศษ !@$%*&	68	48.7

จากตารางที่ 2.3 เมื่อเทียบกับมาตรฐานการกำหนดรหัสผ่านเว็บไซต์ของ NIST และ PCI DSS แล้ว จะได้ค่า PCP Strength ตามมาตรฐาน NIST คือ 26.6 และค่า PCP Strength ตามมาตรฐาน PCI DSS คือ 36.2

2.3 การตรวจสอบเว็บไซต์ยินยอมให้กำหนดรหัสผ่านที่ไม่ปลอดภัย

เนื่องจากนโยบายการกำหนดรหัสผ่านมีความแตกต่างกันในแต่ละเว็บไซต์ จะทราบได้อย่างไรว่าเว็บไซต์ที่ใช้บริการมีนโยบายการกำหนดรหัสผ่านที่ปลอดภัย ผู้วิจัยได้ศึกษาวิธีตรวจสอบเว็บไซต์ ที่ยินยอมให้กำหนดรหัสผ่านที่ไม่ปลอดภัย [12][20] ได้ทำการสำรวจว่าแต่ละเว็บไซต์ยินยอมให้กำหนดรหัสผ่านที่ไม่ปลอดภัยหรือไม่ โดยอ้างอิงนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST ซึ่งงานวิจัยดังกล่าวสำรวจตามนโยบายแต่ละข้อดังนี้

- ห้ามใช้รหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษร
- ห้ามใช้รหัสผ่านซ้ำกับรหัสเดิม 4 ครั้งก่อนหน้า
- ห้ามใช้รหัสผ่านที่เคยพบว่ารั่วไหล [16]
- ห้ามใช้รหัสผ่านที่เดาง่าย
- ต้องมีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด
- ต้องมีการใช้ MFA

งานวิจัย [12] ได้ทำการตรวจสอบนโยบายการกำหนดรหัสผ่านเว็บไซต์ 120 เว็บไซต์ในประเทศสหรัฐอเมริกาอ้างอิงนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST และผลการวิจัยพบข้อมูลดังนี้

- มีเพียงร้อยละ 13 เท่านั้นที่ปฏิบัติตามมาตรฐานดังกล่าว
- ร้อยละ 75 ยินยอมให้ผู้ใช้บริการเว็บไซต์สามารถกำหนดรหัสผ่านที่พบบ่อยที่สุด เช่น “abc123456” และ “P@$$w0rd”
- ร้อยละ 45 บังคับให้กำหนดอักขระพิเศษในรหัสผ่านถึงแม้ว่า NIST จะปรับปรุงมาตรฐานให้ยกเลิกข้อกำหนดดังกล่าวแล้ว โดยควรกำหนดรหัสผ่านที่มีความยาวอย่างน้อย 8 ตัวอักษร และไม่ควรมีข้อกำหนดระดับอักขระเพื่อให้ผู้ใช้สามารถตั้งรหัสผ่านที่จำได้และไม่จำเป็นต้องเพิ่มอักขระที่เดาง่าย เช่นเติมเครื่องหมาย “!” เป็นตัวสุดท้ายของรหัสผ่านเพื่อให้เป็นไปตามข้อกำหนดของเว็บไซต์

งานวิจัย [20] ได้ทำการตรวจสอบนโยบายการกำหนดรหัสผ่านเว็บไซต์ในประเทศสหรัฐอเมริกาโดยใช้ Verizon DBIR เป็นจุดเริ่มต้นในการระบุอุตสาหกรรมที่มีจำนวนเหตุการณ์ด้านความปลอดภัยทางไซเบอร์มากที่สุด ข้อมูลถูกรวบรวมจาก 108 เว็บไซต์ที่สุ่มเลือกภายใน 9 อุตสาหกรรมที่ทราบกันดีว่ามีเหตุการณ์ด้านความปลอดภัยทางไซเบอร์เกิดขึ้นบ่อยครั้ง โดยศึกษาอ้างอิงนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST ในแต่ละหัวข้อ และผลการวิจัยพบข้อมูลดังนี้

- เกือบทุกเว็บไซต์ (มากกว่าร้อยละ 95) ปฏิบัติตามคำแนะนำของ NIST หัวข้อการใช้ 2FA
- เว็บไซต์ส่วนใหญ่ (ร้อยละ 76) ปฏิบัติตามคำแนะนำของ NIST หัวข้อความซับซ้อนของรหัสผ่าน
- เว็บไซต์มากกว่าครึ่ง (ร้อยละ 61) ปฏิบัติตามคำแนะนำของ NIST หัวข้อความยาวขั้นต่ำของรหัสผ่าน
- เว็บไซต์มากกว่าครึ่ง (ร้อยละ 59) ปฏิบัติตามคำแนะนำของ NIST หัวข้อมีการล็อคบัญชีผู้ใช้
- เว็บไซต์ส่วนน้อย (ร้อยละ 19) ปฏิบัติตามคำแนะนำของ NIST หัวข้อห้ามใช้รหัสผ่านที่เดาง่าย ในขณะที่ร้อยละ 81 ยอมให้กำหนดรหัสผ่านเป็น “P@ssw0rd” ได้

2.4 การตรวจสอบเว็บไซต์ที่ถูกพบ Data Breach

เรามักเห็นข่าวเกี่ยวกับเว็บไซต์ถูกพบ data breach อยู่เป็นระยะ ซึ่งบางครั้งส่งผลกระทบให้ข้อมูลผู้ใช้บริการเว็บไซต์รั่วไหล และถูกเข้าถึงอย่างไม่ถูกต้อง เราจะทราบได้อย่างไรว่าเว็บไซต์ที่ใช้บริการเคยถูกพบปัญหา data breach หรือไม่ ผู้วิจัยได้ศึกษาวิธีตรวจสอบเว็บไซต์ที่ถูกพบ Data Breach [15] ที่ทำการสำรวจกลุ่มตัวอย่างเว็บไซต์ในประเทศสหรัฐอเมริกาและประเทศเยอรมณี ซึ่งส่วนหนึ่งของการศึกษาได้ทำการสำรวจว่าแต่ละเว็บไซต์เคยพบปัญหา Data Breach หรือไม่ โดยใช้ Google search engine ค้นหาชื่อเว็บไซต์ร่วมกับข้อความดังนี้

- password breach
- password leak
- password hack
- password incident

หากผลการค้นหาแสดงเว็บไซต์ที่มีข้อมูลว่าเคยพบปัญหา Data Breach แสดงผลในหน้าแรกของผลการค้นหาจะถือว่าเว็บไซต์ดังกล่าวเคยพบปัญหา data breach

2.5 ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล คือข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม โดยข้อมูลของผู้ถึงแก่กรรม และข้อมูลนิติบุคคล ไม่ถือเป็นข้อมูลส่วนบุคคลตาม พ.ร.บ. PDPA คุ้มครองข้อมูลส่วนบุคคลนี้ [1] ข้อมูลส่วนบุคคล (Personal Data) ได้แก่

- ชื่อ - นามสกุล
- เลขประจำตัวประชาชน
- ที่อยู่
- เบอร์โทรศัพท์
- วันเกิด
- อีเมล
- การศึกษา
- เพศ
- อาชีพ
- รูปถ่าย
- ข้อมูลทางการเงิน

นอกจากนี้ยังรวมถึง ข้อมูลส่วนบุคคลที่มีความละเอียดอ่อน (Sensitive Personal Data) ด้วย เช่น ข้อมูลทางการแพทย์หรือสุขภาพ, ข้อมูลทางพันธุกรรมและไบโอเมทริกซ์, เชื้อชาติ, ความคิดเห็นทางการเมือง, ความเชื่อทางศาสนาหรือปรัชญา, พฤติกรรมทางเพศ, ประวัติอาชญากรรม, ข้อมูลสหภาพแรงงาน เป็นต้น

2.6 นโยบายในการกำหนดรหัสผ่านตามมาตรฐานของ สกมช.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีผลใช้บังคับเมื่อวันที่ 28 พฤษภาคม 2562 โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ และประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

ปัจจุบัน สกมช. ได้กำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์ (Website Security Guideline) เพื่อให้คำแนะนำหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีการจัดทำเว็บไซต์ [3] ซึ่งในหัวข้อ 4.6 กล่าวถึงการทำให้เว็บแอปพลิเคชันมีความปลอดภัย (Secure web applications) โดยระบุและลดความเสี่ยงของการถูกโจมตีบนเว็บแอปพลิเคชันที่สำคัญ ๑๐ อันดับแรก (ข้อมูลเพิ่มเติมเกี่ยวกับความเสี่ยง ๑๐ อันดับแรกจาก OWASP3 จากนั้นจึงพิจารณาระบุและลดความเสี่ยงอื่น ๆ เป็นลำดับถัดไป อาทิ การปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยของระบบและเครือข่ายที่มีการใช้งานเทคโนโลยีอินเทอร์เน็ตจาก Center for Internet Security (CIS) ซึ่งในส่วนของนโยบายการกำหนดความยาวของรหัสผ่านควรพัฒนาตามมาตรฐาน NIST SP800-63B และมีข้อกำหนดเพิ่มเติม สรุปได้ดังนี้

- รหัสผ่านต้องมีความยาวอย่างน้อย 8 ตัวอักษร
- ห้ามใช้รหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรม
- ห้ามใช้รหัสผ่านที่เคยพบว่ารั่วไหล
- มีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด หรือใช้ CAPCHA เพื่อป้องกัน Brute Force Attack
- ต้องใช้ Multi Factor Authentication

2.7 นโยบายในการกำหนดรหัสผ่านตามมาตรฐานของ NIST

National Institute of Standards and Technology หรือ NIST เป็นหน่วยงานหนึ่งของกระทรวงพาณิชย์สหรัฐอเมริกา ที่รักษามาตรฐานความปลอดภัย เพื่อปกป้องระบบขององค์กร มีจุดประสงค์หลักคือการส่งเสริมนวัตกรรมและการแข่งขันในอุตสาหกรรม ให้มีความก้าวหน้าทางวิทยาศาสตร์ มีการวัดมาตรฐานและเทคโนโลยีในเพื่อเพิ่มความมั่นคงทางเศรษฐกิจ และปรับปรุง

คุณภาพชีวิตของเราให้ดียิ่งขึ้น โดยปกติการควบคุมความปลอดภัยมาตรฐาน 800-53 ของ NIST จะใช้กับระบบสารสนเทศของรัฐบาลกลางสหรัฐอเมริกา โดยทั่วไประบบสารสนเทศของรัฐบาลกลางจะต้องผ่านการประเมินอย่างเป็นทางการและผ่านกระบวนการให้สิทธิ์อนุญาต เพื่อให้แน่ใจว่ามีการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งานของข้อมูลและระบบข้อมูลที่เพียงพอ เฟรมเวิร์คด้านความมั่นคงปลอดภัยทางไซเบอร์ของ NIST (CSF) ได้รับการสนับสนุนจากรัฐบาลและอุตสาหกรรมต่างๆ ทั่วโลกในฐานะที่เป็นบรรทัดฐานที่แนะนำสำหรับให้องค์กรต่างๆ นำไปใช้ ไม่ว่าจะเป็นภาคส่วนใดหรือมีขนาดเท่าใด จากข้อมูลของ Gartner ในปี 2015 องค์กรในสหรัฐอเมริกา ประมาณ 30 เปอร์เซ็นต์ใช้ CSF และคาดว่าการใช้งานจะเพิ่มขึ้นเป็น 50 เปอร์เซ็นต์ในปี 2020 ตั้งแต่ปีงบประมาณ 2016 มีการนำตัววัด Federal Information Security Modernization Act (FISMA) ของรัฐบาลกลางมาใช้จัดการ CSF และขณะนี้หน่วยงานของรัฐบาลต้องใช้ CSF ภายใต้ Cybersecurity Executive Order [17] โดยส่วนหนึ่งของมาตรฐานคือนโยบายในการกำหนดรหัสผ่านที่ควรปฏิบัติตามดังนี้

- รหัสผ่านต้องมีความยาวอย่างน้อย 8 ตัวอักษร
- ห้ามใช้รหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษร เช่น 12345, aaaaa
- ห้ามใช้รหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรม
- ห้ามใช้รหัสผ่านที่เคยพบว่ารั่วไหล
- มีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด
- ต้องใช้ Multi Factor Authentication (MFA) เมื่อมีการขอข้อมูลส่วนบุคคล

2.8 นโยบายในการกำหนดรหัสผ่านตามมาตรฐานของ PCI DSS

PCI DSS คือมาตรฐานความปลอดภัยของข้อมูลบัตรชำระเงิน ที่เป็นมาตรฐานสากลสำหรับยกระดับมาตรฐานความปลอดภัยข้อมูลบัตรชำระเงิน โดยการควบคุมความปลอดภัยที่จัดการโดย PCI Security Standards Council และพัฒนาโดยผู้เชี่ยวชาญจากหน่วยงานบัตรชำระเงินระหว่างประเทศ (VISA, MasterCard, JCB, AMEX และ Discover) เพื่อช่วยป้องกันการละเมิดข้อมูลบัตรเครดิต มาตรฐานความปลอดภัยข้อมูลนี้มีข้อกำหนดเพื่อช่วยปกป้องข้อมูลผู้ถือบัตร โดยคำนึงถึงคน, กระบวนการและเทคโนโลยีที่เกี่ยวข้องในระบบการประมวลผลบัตรชำระเงิน ซึ่งจะมุ่งเน้นการจัดการความปลอดภัยทั้งนโยบาย ขั้นตอน ระบบและการออกแบบซอฟต์แวร์ที่เชื่อถือได้ โดยส่วนหนึ่งของมาตรฐานคือนโยบายในการกำหนดรหัสผ่านที่ควรปฏิบัติตามดังนี้ [18]

- รหัสผ่านต้องมีความยาวอย่างน้อย 7 ตัวอักษร
- รหัสผ่านต้องประกอบด้วยตัวเลขและตัวอักษรภาษาอังกฤษ

- เปลี่ยนรหัสผ่านทุก 90 วัน และรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสผ่าน 4 ครั้งก่อนหน้า
- ห้ามใช้รหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรม
- ห้ามใช้รหัสผ่านที่เคยพบว่ารั่วไหล
- ต้องมีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด
- ต้องใช้ Multi Factor Authentication (MFA)

2.9 การคัดเลือกกลุ่มตัวอย่างเว็บไซต์

จากงานวิจัยก่อนหน้าที่ทำการศึกษาและเปรียบเทียบนโยบายการกำหนดรหัสผ่านของเว็บไซต์แต่ละประเภทในประเทศสหรัฐอเมริกา ประเทศเยอรมนี และประเทศไทย [8] ผลการศึกษาพบว่าเว็บไซต์หน่วยงานรัฐไทยมีนโยบายการกำหนดรหัสผ่านที่ต่ำกว่าประเทศสหรัฐอเมริกาและประเทศเยอรมนี แม้จะมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลบังคับใช้ในประเทศไทย[19] หลังประกาศใช้กฎหมายดังกล่าวพบเพียง 2 จาก 10 หน่วยงานที่ปรับนโยบายการกำหนดรหัสผ่านให้มีความปลอดภัยมากขึ้น ถึงแม้ว่าเว็บไซต์เหล่านั้นมีการเก็บข้อมูลส่วนบุคคลของผู้ใช้งานก็ตาม จากข้อมูลข้างต้นผู้วิจัยจึงเลือกเว็บไซต์หน่วยงานรัฐไทยเป็นหนึ่งในกลุ่มตัวอย่างเว็บไซต์

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เผยผลสำรวจมูลค่าพาณิชย์อิเล็กทรอนิกส์ในประเทศไทย พบว่าในปีพ.ศ. 2563 ประเทศไทยครองแชมป์มูลค่าอีคอมเมิร์ซแบบ B2C สูงสุดในกลุ่มประเทศอาเซียนติดต่อกัน 7 ปีซ้อน และคาดการณ์ว่าปีพ.ศ. 2564 จะมีแนวโน้มการเติบโตอย่างต่อเนื่องภายหลังจากการฟื้นตัวจากสถานการณ์โรคระบาดโควิด-19 โดยคาดการณ์ว่าเติบโตร้อยละ 6.11 จากปีพ.ศ. 2563 [4]

SimilarWeb คือบริษัทที่ให้ให้บริการด้าน Web Analytic Service จากประเทศอิสราเอล โดยมีความสามารถในการวิเคราะห์/ติดตามปริมาณ Traffic Website ซึ่งสามารถระบุไว้ว่ามาจากประเทศใดมีสัดส่วนเท่าใด และจากสถิติเว็บไซต์ที่มีผู้เข้าชมมากที่สุดทุกหมวดหมู่ในประเทศไทยเดือนเมษายนปีพ.ศ. 2566 [22] พบว่าเว็บไซต์อีคอมเมิร์ซมีผู้เข้าชมอยู่ใน 20 อันดับแรกถึงสองเว็บไซต์ จากข้อมูลสถิติดังกล่าวผู้วิจัยจึงเลือกเว็บไซต์ที่ให้บริการซื้อขายสินค้าเป็นหนึ่งในกลุ่มตัวอย่างเว็บไซต์

จากข้อมูลสถิติอัตราการเข้าพักของสถานพักแรมทั่วประเทศ โดยธนาคารแห่งประเทศไทย [2] พบว่าในปีพ.ศ. 2564 อัตราการเข้าพักของสถานพักแรมอยู่ที่ร้อยละ 14.02 หลังจากผ่อนปรนมาตรการโควิด-19 อัตราการเข้าพักของสถานพักแรมอยู่ที่ร้อยละ 47.94 และข้อมูลล่าสุด 3 เดือนแรกของปีพ.ศ. 2566 อัตราการเข้าพักของสถานพักแรมอยู่ที่ร้อยละ 70.28 ซึ่งเห็นได้อย่างชัดเจนว่าธุรกิจการโรงแรมและการท่องเที่ยวเติบโตขึ้นเป็นอย่างมาก และปัจจุบันการจองห้องพักโรงแรมรวมถึงการจองตั๋ว

เครื่องบินโดยสารสามารถดำเนินการผ่านเว็บไซต์ได้อย่างง่ายดาย และสามารถชำระค่าบริการผ่านเว็บไซต์ได้ จากข้อมูลสถิติดังกล่าวผู้วิจัยจึงเลือกเว็บไซต์ด้านการโรงแรมและการท่องเที่ยวเป็นหนึ่งในกลุ่มตัวอย่างเว็บไซต์

2.10 ช่องทางการชำระเงินผ่านเว็บไซต์ในประเทศไทย

ปัจจุบันเว็บไซต์ผู้ให้บริการด้านอีคอมเมิร์ซ ด้านโรงแรมและการท่องเที่ยว หรือเว็บไซต์อื่นๆ ที่มีระบบชำระเงินผ่านเว็บไซต์ ได้เพิ่มความสะดวกให้กับผู้ใช้บริการสามารถชำระเงินได้หลากหลายช่องทางมากขึ้น จากเดิมหากต้องการชำระค่าสินค้าหรือบริการผ่านเว็บไซต์ ผู้ใช้บริการต้องคัดลอกข้อมูลเพื่อนำไปชำระเงินผ่านสาขาธนาคาร หรือผ่านแอพพลิเคชั่นของธนาคาร แต่ในปัจจุบันช่องทางการชำระเงินผ่านเว็บไซต์มีให้เลือกใช้มากมาย เช่น จ่ายผ่าน QR Promptpay, จ่ายผ่าน e-Wallet, จ่ายผ่านแอพพลิเคชั่นของธนาคาร, ส่งรายการเรียกเก็บเงินไปยังแอพพลิเคชั่นของธนาคาร, จ่ายผ่านเลขบัญชีธนาคาร, จ่ายผ่านบัตรเครดิต/เดบิต, จ่ายผ่านเลขอ้างอิง เป็นต้น ซึ่งในการจ่ายเงินแต่ละประเภทผู้ใช้บริการสามารถบันทึกข้อมูลการชำระเงินเพื่อใช้งานได้สะดวกขึ้นในการชำระค่าสินค้าและบริการครั้งถัดไป

จากช่องทางการชำระเงินข้างต้น เกือบทั้งหมดต้องใช้อุปกรณ์อื่นในการชำระเงิน เช่น กรณีจ่ายผ่าน QR Promptpay ต้องใช้แอพลิเคชันของธนาคารเพื่อทำการชำระเงิน กรณีจ่ายผ่าน e-Wallet ต้องใช้แอพพลิเคชั่น wallet ในการชำระเงิน เป็นต้น แต่สำหรับการจ่ายด้วยบัตรเครดิต และผู้ใช้บริการสามารถบันทึกข้อมูลบัตรเครดิตในระบบได้ และผู้ใช้บริการสามารถเรียกดูรายระเอียดบัตรเครดิตเมื่อเข้าสู่ระบบ หากบัญชีผู้ใช้บริการถูกบุคคลอื่นสามารถเข้าถึงบัญชีได้ ก็สามารถเข้าถึงข้อมูลบัตรเครดิตได้เช่นกัน

2.11 การประเมินความเต็มใจของผู้ใช้บริการ

ทฤษฎีความเต็มใจที่จะจ่าย หมายถึงความยินดีหรือความเต็มใจของผู้บริโภคที่พร้อมจะจ่ายค่าสินค้าหรือบริการชนิดใดชนิดหนึ่ง ซึ่งการคำนวณหาความเต็มใจที่จะจ่ายสามารถทำได้ 2 วิธีใหญ่ๆ คือ วิธีการทางตรงที่หมายถึงเป็นการสอบถามผู้ใช้บริการและวิธีการทางอ้อมที่หมายถึงการสังเกตพฤติกรรมของผู้ใช้บริการแล้วนำมาคำนวณเป็นความเต็มใจที่จะจ่าย [7] การจัดระดับความพึงพอใจหรือความคิดเห็น ผ่านแบบสอบถามมีได้หลายระดับ [10] คือ

- วัด 2 ระดับ เช่น ดีหรือไม่ดี เต็มใจหรือไม่เต็มใจ พอใจหรือไม่พอใจ
- วัด 3 ระดับ คือ มาก ปานกลาง น้อย
- วัด 5 ระดับ คือ มากที่สุด มาก ปานกลาง น้อย น้อยที่สุด

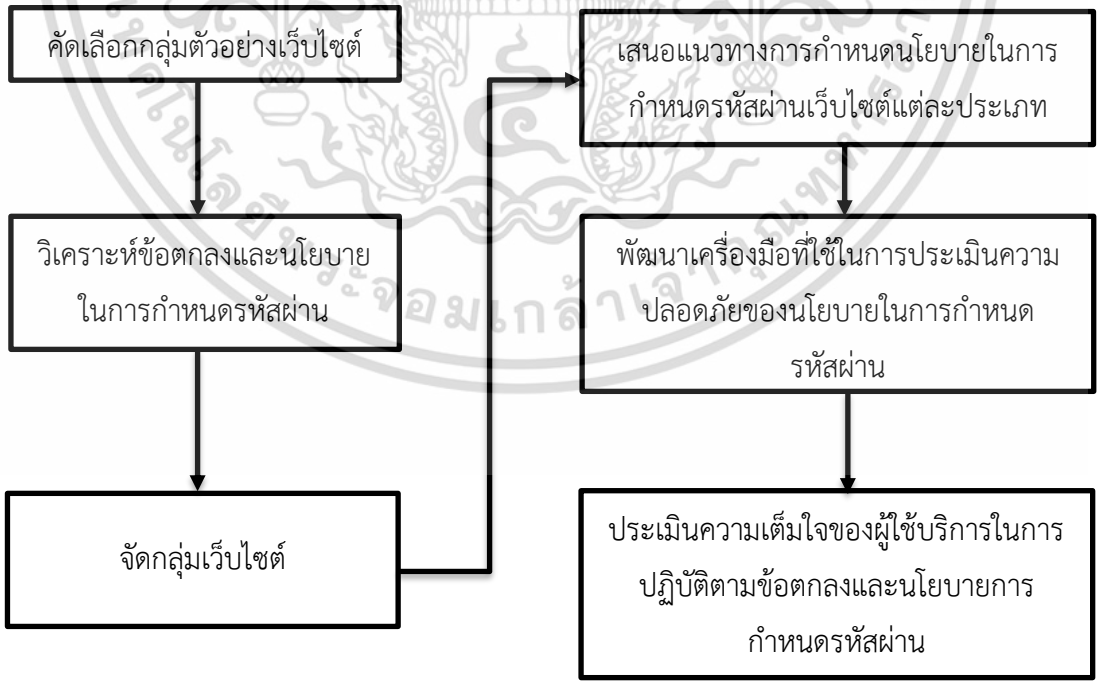
- วัด 7 ระดับ (Semantic Differential Scale) เป็นการให้สเกลคำตอบ 7 ระดับ เช่น รวดเร็ว 7 6 5 4 3 2 1 ล่าช้า หรือ ประทับใจ 7 6 5 4 3 2 1 ไม่ประทับใจ
- วัดแบบ Thurstone’ s Scale ซึ่งมี 11 ระดับ

บทที่ 3

วิธีการดำเนินงานวิจัย

ดังที่ได้กล่าวในบทนำโดยอ้างอิงจากผลงานวิจัยก่อนหน้า ค่า PCP Strength เว็บไซต์ของรัฐไทยให้ค่า PCP Strength ต่ำที่สุดจากกลุ่มตัวอย่างทั้งหมด การใช้งานเว็บไซต์ที่ให้บริการซื้อขายสินค้าเว็บไซต์ด้านการโรงแรมและการท่องเที่ยวที่เพิ่มขึ้นหลังประสบปัญหาโรคระบาดโควิด-19 และปัจจุบันประเทศไทยยังไม่มีการกำหนดนโยบายในการกำหนดรหัสผ่านของเว็บไซต์แต่ละประเภทที่ชัดเจน ทำให้ผู้พัฒนาทำการกำหนดและปรับใช้ตามแต่ละองค์กร ซึ่งผู้พัฒนาและผู้ใช้บริการไม่ได้ตระหนักรู้ถึงความปลอดภัยจากข้อตกลงและนโยบายการกำหนดรหัสผ่านที่ไม่แข็งแรง จึงอาจทำให้ข้อมูลของผู้ใช้บริการรั่วไหล และส่งผลต่อความน่าเชื่อถือของเว็บไซต์

งานวิจัยนี้จึงทำการศึกษาวิจัยเพื่อวิเคราะห์ความปลอดภัยและเปรียบเทียบนโยบายในการกำหนดรหัสผ่านบนเว็บไซต์ในประเทศไทย และเสนอนโยบายในการกำหนดรหัสผ่านเว็บไซต์แต่ละประเภทให้เป็นไปตามมาตรฐานสากล รวมถึงพัฒนาเครื่องมือที่ใช้ในการประเมินความปลอดภัยของนโยบายในการกำหนดรหัสผ่านที่ยังคงตอบโจทย์ผู้ใช้งานและไม่สร้างความยากลำบากจนเกินไป โดยมีขั้นตอนการดำเนินงานดังนี้



3.1 ขั้นตอนการคัดเลือกกลุ่มตัวอย่างเว็บไซต์

3.1.1 เว็บไซต์หน่วยงานรัฐไทย

ผู้วิจัยได้นำข้อมูลจากสำนักงานสถิติแห่งชาติ [5] ซึ่งรวบรวมเว็บไซต์หน่วยงานต่างของภาครัฐทั้งหมด 167 เว็บไซต์ ซึ่งพบว่าบางเว็บไซต์ไม่มีระบบสำหรับให้ประชาชนทั่วไปสมัครเข้าใช้งาน บางเว็บไซต์ที่ประชาชนทั่วไปสามารถสมัครสมาชิกเข้าใช้งานได้เป็นเพียงระบบร้องทุกข์ที่ไม่ต้องการข้อมูลส่วนบุคคล งานวิจัยนี้จึงทำการคัดเลือกเว็บไซต์โดยมีเงื่อนไขคือ ต้องมีระบบสมัครสมาชิกที่ประชาชนทั่วไปสามารถสมัครสมาชิกได้และระบบมีการขอข้อมูลส่วนบุคคลเพื่อเข้าใช้งานระบบ จากเงื่อนไขดังกล่าวจึงเหลือเพียง 20 เว็บไซต์ โดยเรียงลำดับตามยอดผู้เข้าใช้งานดังนี้

ตารางที่ 3.1 เว็บไซต์หน่วยงานรัฐไทยที่ทำการศึกษาวิจัย

ลำดับที่	ชื่อหน่วยงาน	Website URL
1	กรมสรรพากร	www.rd.go.th
2	สำนักงานประกันสังคม	www.sso.go.th
3	กรมการจัดหางาน	www.doe.go.th
4	กรมพัฒนาธุรกิจการค้า	www.dbd.go.th
5	กรมการปกครอง	www.dopa.go.th
6	กรมบังคับคดี	www.led.go.th
7	กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช	www.dnp.go.th
8	กรมศิลปากร	www.finearts.go.th
9	กรมส่งเสริมการเกษตร	www.doae.go.th
10	กรมศุลกากร	www.customs.go.th
11	กรมทางหลวง	www.doh.go.th
12	สำนักงานการปฏิรูปที่ดินเพื่อเกษตรกรรม	www.alro.go.th
13	สำนักงานสถิติแห่งชาติ	www.nso.go.th
14	ศูนย์มนุษยวิทยาสิรินธร	www.sac.or.th
15	กรมปศุสัตว์	www.dld.go.th
16	กรมการค้าภายใน	www.dit.go.th
17	สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ	www.gistda.or.th

ตารางที่ 3.1 เว็บไซต์หน่วยงานรัฐไทยที่ทำการศึกษาวิจัย (ต่อ)

ลำดับที่	ชื่อหน่วยงาน	Website URL
18	สำนักงานคณะกรรมการคุ้มครองผู้บริโภค	www.ocpb.go.th
19	กรมส่งเสริมคุณภาพสิ่งแวดล้อม	www.deqp.go.th
20	สำนักงานคณะกรรมการกองทุนหมู่บ้านและชุมชนเมืองแห่งชาติ	www.villagefund.or.th

3.1.2 เว็บไซต์ที่ให้บริการซื้อขายสินค้า

ผู้วิจัยได้ค้นหาเว็บไซต์ที่มียอดผู้เข้าชมสูงสุดจากระบบ SEMRush [21] ซึ่งเป็นเครื่องมือการทำ Search Engine Optimization สำหรับทำการตลาดเพื่อโปรโมทสินค้าและบริการผ่านสื่อดิจิตอล ระบบดังกล่าวสามารถค้นหาเว็บไซต์ที่มียอดผู้เข้าชมสูงสุด โดยระบบมีช่องทางค้นหาผ่าน API ซึ่งสามารถค้นหาข้อมูลตามช่วงเวลาได้ และสามารถค้นหาฟรีได้มากกว่า 1,000 เว็บไซต์โดยเรียงลำดับตามยอดผู้เข้าชมสูงสุด

จากสถิติเว็บไซต์ที่มียอดผู้เข้าชมสูงสุด 1,000 เว็บไซต์ ผู้วิจัยได้คัดเลือกเว็บไซต์ในหมวดหมู่อีคอมเมิร์ซที่มียอดผู้เข้าชมสูงสุด 5 อันดับแรก และคัดเลือกธุรกิจค้าปลีกที่มูลค่าธุรกิจเกิน 3 พันล้านบาท [23] และให้บริการสั่งซื้อสินค้าผ่านเว็บไซต์ โดยมีเว็บไซต์ที่เข้าเงื่อนไขดังกล่าวดังนี้

ตารางที่ 3.2 เว็บไซต์ที่ให้บริการซื้อขายสินค้าที่ทำการศึกษาวิจัยในกลุ่มอีคอมเมิร์ซ

ลำดับที่	Website URL
1	www.lazada.co.th
2	www.shopee.co.th
3	www.homepro.co.th
4	www.kaidee.com
5	www.thaiwatsadu.com

ตารางที่ 3.3 เว็บไซต์ที่ให้บริการซื้อขายสินค้าที่ทำการศึกษาวิจัยในกลุ่มธุรกิจค้าปลีก

ลำดับที่	Website URL
1	www.shopat24.com
2	www.lotuss.com
3	www.central.co.th
4	www.bigc.com
5	www.makro.com

3.1.3 เว็บไซต์ด้านการโรงแรมและการท่องเที่ยว

ผู้วิจัยได้ทำการค้นหาเว็บไซต์ที่มียอดผู้เข้าชมสูงสุดด้วยวิธีการเดียวกับการค้นหาเว็บไซต์กลุ่มอีคอมเมิร์ซโดยเลือก 10 อันดับแรกที่ให้บริการจองห้องพักโรงแรม และจองตั๋วเครื่องบิน โดยมีเว็บไซต์ที่เข้าเงื่อนไขดังกล่าว เรียงลำดับตามยอดผู้เข้าใช้งานดังนี้

ตารางที่ 3.4 เว็บไซต์ด้านการโรงแรมและการท่องเที่ยวที่ทำการศึกษาวิจัย

ลำดับที่	Website URL
1	www.agoda.com
2	www.airasia.com
3	www.booking.com
4	www.tripadvisor.com
5	www.trip.com
6	www.klook.com
7	www.traveloka.com
8	www.vietjetair.com
9	www.thaiairways.com
10	www.emirates.com

3.2 ขั้นตอนการวิเคราะห์ข้อตกลงและนโยบายในการกำหนดรหัสผ่าน

ผู้วิจัยได้อ้างอิงการศึกษาข้อตกลงและนโยบายในการกำหนดรหัสผ่านเว็บไซต์ [12][20] เพื่อค้นหาว่าเว็บไซต์กำหนดข้อตกลงและนโยบายในการกำหนดรหัสผ่านตามมาตรฐาน NIST และ PCI DSS หรือไม่ โดยปฏิบัติตามขั้นตอนดังนี้

1. สมัครใช้บริการเว็บไซต์
2. ค้นหาความยาวขั้นต่ำของรหัสผ่านและจำนวนอักขระขั้นต่ำที่บังคับจากเอกสาร PCP หรือ hint ของเว็บไซต์
3. กำหนดรหัสผ่านเป็น Hello123 เพื่อตรวจสอบว่ายอมให้ใช้รหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษรหรือไม่
4. กำหนดรหัสผ่านตาม NCSC-HIBP-100k [13] เพื่อตรวจสอบว่ายอมให้ใช้รหัสผ่านที่เคยพบว่าเป็นช่องโหว่และรั่วไหลหรือไม่
5. กำหนดรหัสผ่านตาม Password Guess ability Service [6] เพื่อตรวจสอบว่ายอมให้ใช้รหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรมหรือไม่
6. ตรวจสอบว่าต้องใช้ MFA หรือไม่
7. กำหนดรหัสผ่านให้ตรงตามนโยบายของเว็บไซต์
8. เปลี่ยนรหัสผ่าน 3 ครั้งและเปลี่ยนรหัสผ่านครั้งที่ 4 เหมือนกับรหัสผ่านครั้งแรก เพื่อตรวจสอบว่ายอมให้ใช้รหัสผ่านใหม่ที่ซ้ำกับรหัสผ่าน 4 ครั้งก่อนหน้าหรือไม่
9. ตรวจสอบว่าเว็บไซต์มีการขอข้อมูลส่วนบุคคลหรือไม่
10. ตรวจสอบว่าเว็บไซต์ที่ให้บริการซื้อขายสินค้าผ่านเว็บไซต์ มีช่องทางการชำระเงินแบบใดบ้าง
11. ตรวจสอบเว็บไซต์ที่ให้บริการซื้อขายสินค้าผ่านเว็บไซต์และรับชำระเงินผ่านบัตรเครดิตสามารถเก็บข้อมูลบัตรเครดิตในระบบได้หรือไม่
12. ตรวจสอบเว็บไซต์ที่เก็บข้อมูลบัตรเครดิตในระบบ สามารถเรียกดูข้อมูลบัตรเครดิตที่บันทึกไว้หรือไม่
13. ออกจากระบบ
14. เข้าสู่ระบบโดยระบุรหัสผ่านผิด 6 ครั้ง เพื่อตรวจสอบว่ามีการระงับบัญชีหรือไม่
15. เข้าสู่ Google search engine และทำการค้นหาชื่อเว็บไซต์ร่วมกับข้อความดังนี้ password breach, password leak, password hack, password incident [15] เพื่อตรวจสอบว่าเว็บไซต์เคยถูกพบ data breach หรือไม่

3.3 ขั้นตอนการจัดกลุ่มเว็บไซต์

หลังจากได้ข้อมูลจากหัวข้อ 3.2 จะทำการจัดกลุ่มเว็บไซต์โดยแยกเป็น 3 กลุ่ม เพื่อเสนอแนวทางกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์ที่เหมาะสมต่อไป โดยแบ่งเป็นดังนี้

- เว็บไซต์หน่วยงานรัฐ
- เว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคล และไม่มีการเก็บข้อมูลบัตรเครดิตในระบบ
- เว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคล และมีการเก็บข้อมูลบัตรเครดิตในระบบ

3.4 ขั้นตอนการเสนอแนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์ให้เป็นไปตามมาตรฐานของ NIST และ PCI DSS

ผู้วิจัยดำเนินการศึกษามาตรฐาน NIST SP 800-63B ในหัวข้อที่เกี่ยวกับนโยบายการกำหนดรหัสผ่านที่เหมาะสมกับเว็บไซต์ที่มีการเก็บข้อมูลแต่ละประเภท และศึกษามาตรฐาน PCI DSS 3.2.1 ในหัวข้อที่เกี่ยวกับนโยบายการกำหนดรหัสผ่าน เพื่อนำมาตรฐานดังกล่าวมาเสนอเป็นแนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์ ดังนี้

1. เว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคล จะต้องปฏิบัติตามมาตรฐาน NIST SP 800-63B
2. เว็บไซต์ที่ไม่มีการเก็บข้อมูลส่วนบุคคล จะต้องปฏิบัติตามมาตรฐาน NIST SP 800-63B
3. เว็บไซต์ที่มีการเก็บข้อมูลบัตรเครดิต จะต้องปฏิบัติตามมาตรฐาน PCI DSS 3.2.1

3.5 ขั้นตอนการพัฒนาแนวปฏิบัติที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่านสำหรับผู้พัฒนาระบบ

ผู้วิจัยจะดำเนินการพัฒนาเว็บไซต์สำหรับกำหนดรหัสผ่านโดยปฏิบัติตามมาตรฐาน NIST SP 800-63B และ PCI DSS 3.2.1 โดยระบุถึงข้อมูลที่จัดเก็บในระบบให้ผู้ใช้งานทราบ และให้ผู้ใช้ดำเนินการกำหนดรหัสผ่าน เพื่อเป็นแนวทางให้ผู้ใช้งานนำไปปรับใช้กับการกำหนดรหัสผ่านเว็บไซต์ที่ใช้งานอยู่ในปัจจุบันได้อย่างปลอดภัย

3.6 ขั้นตอนการประเมินความเต็มใจของผู้ใช้บริการในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST และ PCI DSS

หลังจากศึกษามาตรฐาน NIST และ PCI DSS และสามารถเสนอแนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์ ผู้วิจัยได้นำทฤษฎีความเต็มใจที่จะจ่าย และการจัดระดับความพึงพอใจหรือความคิดเห็นมาปรับใช้กับงานวิจัย โดยเลือกใช้วิธีการสอบถามโดยตรงกับผู้ใช้บริการผ่านแบบสอบถามออนไลน์ ซึ่งจัดระดับความยากง่ายในการปฏิบัติตามนโยบายการกำหนดรหัสผ่านแต่ละข้อ และความ

เต็มใจที่จะปฏิบัติตามการเสนอแนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์ให้เป็นไปตามมาตรฐานของ NIST และ PCI DSS เพื่อประเมินความเต็มใจของผู้ใช้บริการ หากให้ผู้บริการเว็บไซต์นำไปใช้กับนโยบายการกำหนดรหัสผ่านปัจจุบันให้เป็นไปตามมาตรฐาน โดยได้จัดทำแบบสอบถามสำรวจผู้ใช้งานเว็บไซต์ โดยสอบถามว่าสามารถปฏิบัติตามนโยบายทั้งหมดได้อย่างเต็มใจเพื่อความปลอดภัยของผู้ใช้บริการเว็บไซต์ และนโยบายข้อใดที่สามารถปฏิบัติตามได้ยากหรือง่าย เพื่อประเมินนโยบายที่นำเสนอว่าสามารถนำไปใช้ได้จริงโดยที่ผู้ใช้งานยังคงยอมรับและเต็มใจใช้บริการมากน้อยเพียงใด

บทที่ 4
ผลการวิจัยและการอภิปรายผล

จากการวิเคราะห์ความปลอดภัยและเปรียบเทียบนโยบายในการกำหนดรหัสผ่านบนเว็บไซต์หน่วยงานรัฐบาล เว็บไซต์ที่ให้บริการซื้อขายสินค้า และเว็บไซต์ด้านโรงแรมและการเดินทางในประเทศไทย โดยอ้างอิงตามมาตรฐานของ สกมช. NIST และ PCI DSS จากกลุ่มตัวอย่างทั้งหมด 40 เว็บไซต์ พบว่ามีเว็บไซต์ที่มีการเก็บข้อมูลหมายเลขบัตรเครดิตจำนวน 16 เว็บไซต์ และเว็บไซต์ที่ไม่มีการเก็บข้อมูลหมายเลขบัตรเครดิตแต่มีการเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการจำนวน 24 เว็บไซต์

เว็บไซต์ที่ไม่มีการเก็บข้อมูลหมายเลขบัตรเครดิตแต่มีการเก็บข้อมูลส่วนบุคคล วิเคราะห์โดยอ้างอิงจากมาตรฐาน สกมช. และ NIST พบว่ามีเพียง 13 จาก 24 เว็บไซต์ที่ปฏิบัติตามคำแนะนำในหัวข้อการกำหนดความยาวขั้นต่ำ 8 ตัวอักษร และเป็นเรื่องน่าตกใจอีกเช่นกันที่พบว่าเว็บไซต์สำนักงานประกันสังคมที่เคยถูกพบปัญหา data breach ยังคงยินยอมให้ผู้ใช้งานสามารถกำหนดรหัสผ่านที่มีความยาว 6 ตัวอักษรและสามารถระบุเพียงตัวเลขอย่างเดียวได้ รหัสผ่านที่สามารถคาดเดาได้ง่ายเช่น Hello123, password ก็สามารถกำหนดได้ ทั้งที่ระบบดังกล่าวมียอดผู้เข้าใช้งานสูงถึง 1,643,003 ครั้งต่อเดือนในช่วงปีที่ผ่านมา อีกทั้งยังเป็นเว็บไซต์ที่มียอดผู้เข้าใช้งานลำดับที่ 2 ในกลุ่มเว็บไซต์หน่วยงานรัฐ

ผลการศึกษาเว็บไซต์ที่มีการเก็บข้อมูลหมายเลขบัตรเครดิตปฏิบัติตามมาตรฐาน PCI DSS ในหัวข้อการกำหนดความยาวและจำนวนอักขระขั้นต่ำที่ควรกำหนดให้มีความยาวอย่างน้อย 7 ตัวอักษร โดยต้องประกอบด้วยตัวเลขและตัวอักษรภาษาอังกฤษ พบว่ามีเพียง 9 จาก 16 เว็บไซต์เท่านั้นที่ปฏิบัติตามคำแนะนำดังกล่าว และยังพบข้อมูลที่น่าตกใจคือเว็บไซต์ agoda.com ซึ่งเคยถูกพบปัญหา data breach ยังคงยินยอมให้ผู้ใช้งานสามารถกำหนดรหัสผ่านที่มีความยาว 8 ตัวอักษรและสามารถระบุเพียงตัวเลขอย่างเดียวได้ รวมถึงสามารถกำหนดรหัสผ่านที่สามารถคาดเดาได้ง่ายเช่น Hello123, password ได้อีกด้วย โดยเว็บไซต์นี้ให้บริการจองห้องพักโรงแรมโดยสามารถชำระเงินผ่านการตัดบัตรเครดิตที่บันทึกในระบบ และมียอดผู้เข้าใช้งานสูงถึง 2,170,031 ครั้งต่อเดือนในปีที่ผ่านมา อีกทั้งยังเป็นเว็บไซต์ที่มียอดผู้เข้าใช้งานสูงที่สุดในกลุ่มเว็บไซต์ด้านโรงแรมและการเดินทางในประเทศไทย สำหรับเว็บไซต์อื่นที่มีการเก็บข้อมูลหมายเลขบัตรเครดิตได้รวบรวมผลการศึกษาดังที่แสดงในตารางที่ 4.1

ตารางที่ 4.1 นโยบายในการกำหนดรหัสผ่านเว็บไซต์ในประเทศไทย

Website/Parameter	ความยาวขั้นต่ำ	อักขระที่บังคับ	PCP Strength	A1	A2	A3	A4	A5	A6	MFA	ช่องทางการชำระเงินที่รองรับ*	เก็บเลขบัตรเครดิต
กรมสรรพากร	8	62	47.6	N	N	N	N	N	Y	Y	CC, ATM, IB, MB, C	N
สำนักงานประกันสังคม	6	10	19.9	N	N	N	N	N	Y	N	N	N
กรมการจัดหางาน	8	36	41.4	N	N	N	N	N	N	N	N	N
กรมพัฒนาธุรกิจการค้า	8	62	47.6	N	N	N	N	N	Y	N	N	N
กรมการปกครอง	8	62	47.6	N	N	N	N	N	N	N	N	N
กรมบังคับคดี	8	62	47.6	N	N	N	N	N	N	N	N	N
กรมอุทยานแห่งชาติ สัตว์ป่าและพันธุ์พืช	6	10	19.9	N	N	N	N	N	N	N	C, ATM	N
กรมศิลปากร	6	10	19.9	N	N	N	N	N	N	N	R	N
กรมส่งเสริมการเกษตร	6	10	19.9	N	N	N	N	N	N	N	N	N
กรมศุลกากร	8	44	43.7	N	N	N	N	N	N	N	N	N
กรมทางหลวง	4	10	13.3	N	N	N	N	N	N	N	N	N
สำนักงานการปฏิรูปที่ดินเพื่อเกษตรกรรม	8	10	26.6	N	N	N	N	N	N	N	N	N

ตารางที่ 4.1 นโยบายในการกำหนดรหัสผ่านเว็บไซต์ในประเทศไทย (ต่อ)

Website/Parameter	ความยาวขั้นต่ำ	อักขระที่บังคับ	PCP Strength	A1	A2	A3	A4	A5	A6	MFA	ช่องทางการชำระเงินที่รองรับ*	เก็บเลขบัตรเครดิต
สำนักงานสถิติแห่งชาติ	8	10	26.6	N	N	N	N	N/A	N	N	N	N
ศูนย์มานุษยวิทยาสิรินธร	6	10	19.9	N	N	N	N	N	N	N	QR, B, AC	N
กรมปศุสัตว์	6	10	19.9	N	N	N	N	N/A	N	N	N	N
กรมการค้าภายใน	1	10	3.3	N	N	N	N	N	N	N	N	N
สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ	6	10	19.9	N	N	N	N	N	N	N	CC, AC	N
สำนักงานคณะกรรมการคุ้มครองผู้บริโภค	8	10	26.6	N	N	N	N	N	N	N	N	N
กรมส่งเสริมคุณภาพสิ่งแวดล้อม	8	10	26.6	N	N	N	N	N	N	N	N	N
สำนักงานคณะกรรมการกองทุนหมู่บ้านและชุมชนเมืองแห่งชาติ	8	10	26.6	N	N	N	N	N	N	N	N	N

ตารางที่ 4.1 นโยบายในการกำหนดรหัสผ่านเว็บไซต์ในประเทศไทย (ต่อ)

Website/Parameter	ความยาวขั้นต่ำ	อักขระที่บังคับ	PCP Strength	A1	A2	A3	A4	A5	A6	MFA	ช่องทางการชำระเงินที่รองรับ*	เก็บเลขบัตรเครดิต
lazada.co.th	8	73	49.5	N	Y	N	N	N	Y	Y	W, R, CC, AC, MB, IB	Y
shopee.co.th	8	52	45.6	N	Y	N	N	N	Y	Y	QR, W, CC, MB	Y
homepro.co.th	6	10	19.9	N	Y	N	N	N	N	N	QR, W, CC	Y
kaidee.com	6	36	31.0	N	N	N	N	N	N	N	N	N
thaiwatsadu.com	6	10	19.9	N	Y	N	N	N	N	N	QR, CC	Y
shopat24.com	6	68	36.5	N	N	N	N	N	N	N	QR, W, CC, IB	Y
lotuss.com	8	62	47.6	N	N	N	N	N	N	N	CC	Y
central.co.th	8	62	47.6	N	N	N	N	N	N	N	CC, QR, B, W	Y
bigc.co.th	6	62	35.7	N	N	N	N	N/A	N	N	CC	Y
makro.pro	6	73	37.1	N	N	N	N	N/A	N	N	QR, W, CC	N
agoda.com	8	10	26.6	N	Y	N	N	N	Y	N	CC, QR, MB, W, C	Y
airasia.com	8	62	47.6	N	Y	N	N	N	Y	N	CC, C, MB, ATM	Y

ตารางที่ 4.1 นโยบายในการกำหนดรหัสผ่านเว็บไซต์ในประเทศไทย (ต่อ)

Website/Parameter	ความยาวขั้นต่ำ	อักขระที่บังคับ	PCP Strength	A1	A2	A3	A4	A5	A6	MFA	ช่องทางการชำระเงินที่รองรับ*	เก็บเลขบัตรเครดิต
booking.com	10	62	59.5	N	Y	N	N	N	Y	N	CC, PayPal	Y
tripadvisor.com	10	41	53.6	N	N	N	N	N	Y	N	CC	Y
trip.com	8	67	48.5	N	Y	N	N	N	N	N	CC	Y
klook.com	8	66	48.4	N	Y	N	N	N	Y	N	CC	Y
traveloka.com	8	10	26.6	N	Y	N	N	N	N	N	CC	Y
vietjetair.com	8	62	47.6	N	N	N	N	N	N	N	QR, W, CC	N
thaiairways.com	8	36	41.4	N	N	N	N	N	N	Y	N	N
emirates.com	8	62	47.6	N	Y	N	Y	Y	N	N	CC	Y

ความหมายของข้อความในตาราง

A1 หมายถึง ห้ามใช้รหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษร

A2 หมายถึง มีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด

A3 หมายถึง ห้ามใช้รหัสผ่านที่เดาง่าย

A4 หมายถึง ห้ามใช้รหัสผ่านที่เคยพบว่ารั่วไหล

A5 หมายถึง ห้ามใช้รหัสผ่านซ้ำกับรหัสผ่าน 4 ครั้งก่อนหน้า

A6 หมายถึง เคยพบปัญหา Data Breach

MFA หมายถึง ต้องใช้ multi factor authentication ในการ login

ช่องทางการชำระเงินที่รองรับ ได้แก่ Credit Card (CC), e-Wallet (W), QR Payment (QR), Reference (R), Counter (C), Branch (B), Account No. (AC), Internet Banking (IB), Mobile Banking (MB) โดยการชำระด้วยเงินสดจะไม่ระบุในตาราง

4.1 ผลการวิเคราะห์ความแข็งแรงของนโยบายรหัสผ่านของเว็บไซต์ในประเทศไทยเปรียบเทียบกับมาตรฐาน สกมช. และ NIST

จากตารางที่ 4.1 เมื่อเปรียบเทียบกับมาตรฐานของ สกมช. และ NIST หัวข้อความยาวขั้นต่ำของรหัสผ่านพบว่ามีเว็บไซต์ที่บังคับผู้ใช้งานกำหนดรหัสผ่านให้มีความยาวอย่างน้อย 8 ตัวอักษรเพียง 13 จากทั้งหมด 24 เว็บไซต์ โดยเว็บไซต์ในกลุ่มอีคอมเมิร์ซและเว็บไซต์ด้านการโรงแรมและการท่องเที่ยวที่ไม่มีการเก็บหมายเลขบัตรเครดิตแต่มีการเก็บข้อมูลส่วนบุคคลของผู้ใช้บริการ จะรวบรวมอยู่ในเว็บไซต์ที่ควรปฏิบัติตามมาตรฐาน NIST โดย 24 เว็บไซต์ดังกล่าวคือ kaidee.com, makro.pro, vietjetair.com, thaiairways.com และเว็บไซต์หน่วยงานรัฐทั้งหมด

ผลการวิเคราะห์พบว่านอกจาก 13 เว็บไซต์ที่ปฏิบัติตามมาตรฐาน NIST ในหัวข้อความยาวขั้นต่ำของรหัสผ่านแล้ว เว็บไซต์อื่นที่ไม่ได้ปฏิบัติตามมาตรฐานมีข้อบังคับการกำหนดความยาวรหัสผ่านขั้นต่ำ 8 ตัวอักษร มีนโยบายที่แตกต่างกันดังนี้

- เว็บไซต์บังคับให้ระบุความยาวรหัสผ่านอย่างน้อย 6 ตัวอักษร มีทั้งหมด 9 เว็บไซต์คือ เว็บไซต์สำนักงานประกันสังคม, เว็บไซต์กรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช, เว็บไซต์กรมศิลปากร, เว็บไซต์กรมส่งเสริมการเกษตร, เว็บไซต์ศูนย์มนุษยวิทยาสิรินธร, เว็บไซต์กรมปศุสัตว์, เว็บไซต์สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ, kaidee.com และ makro.pro
- เว็บไซต์บังคับให้ระบุความยาวรหัสผ่านอย่างน้อย 4 ตัวอักษร คือเว็บไซต์กรมทางหลวง
- เว็บไซต์บังคับให้ระบุความยาวรหัสผ่านอย่างน้อย 1 ตัวอักษร คือเว็บไซต์กรมการค้าภายใน

สำหรับมาตรฐาน สกมช. และ NIST ในหัวข้อต้องใช้ MFA ในการเข้าสู่ระบบ พบว่ามีเว็บไซต์หน่วยงานรัฐเพียงหน่วยงานเดียวที่ปฏิบัติตามมาตรฐานดังกล่าวคือเว็บไซต์กรมสรรพากร ที่ต้องระบุ OTP ทุกครั้งที่มีการเข้าใช้งานระบบ โดยเริ่มบังคับใช้หลังประเทศไทยออกกฎหมายคุ้มครองข้อมูลส่วนบุคคล นอกจากเว็บไซต์กรมสรรพากร เราพบว่า thaiairways.com ต้องระบุ OTP ที่ได้รับผ่าน e-mail ที่สมัครใช้บริการเมื่อต้องทำการเข้าสู่ระบบทุกครั้งเช่นเดียวกัน

เมื่อเปรียบเทียบตามมาตรฐาน สกมช. ไม่มีเว็บไซต์หน่วยงานรัฐใดปฏิบัติตามมาตรฐานในหัวข้อดังต่อไปนี้

- ห้ามใช้รหัสผ่านที่เดาง่าย
- มีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด

เมื่อเปรียบเทียบตามมาตรฐาน NIST เว็บไซต์ kaidee.com, makro.pro, vietjetair.com และ thaiairways.com ไม่ได้ปฏิบัติตามมาตรฐานในหัวข้อดังต่อไปนี้

- ห้ามใช้รหัสผ่านที่เดาง่าย
- มีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด
- ห้ามใช้รหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษร

จากการศึกษาพบว่ามี 5 เว็บไซต์ของหน่วยงานรัฐที่สามารถชำระเงินผ่านเว็บไซต์ได้คือ เว็บไซต์กรมสรรพากร, เว็บไซต์กรมอุทยานแห่งชาติ สัตว์ป่าและพันธุ์พืช, เว็บไซต์กรมศิลปากร, เว็บไซต์ศูนย์มนุษยวิทยาสิรินธร และเว็บไซต์สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ โดยให้บริการดังนี้

- เว็บไซต์กรมสรรพากร เปิดให้ผู้ใช้บริการสามารถชำระภาษีผ่านช่องทางการชำระเงินที่กำหนด โดยรองรับการชำระเงินแบบตัดบัตรเครดิตแต่ไม่สามารถบันทึกข้อมูลบัตรเครดิตในระบบได้
- เว็บไซต์กรมอุทยานแห่งชาติ สัตว์ป่าและพันธุ์พืช เปิดให้ผู้ใช้บริการสามารถจองห้องพักที่อุทยานแห่งชาติได้ โดยสามารถชำระเงินได้ 2 ช่องทางคือ ชำระเงินที่หน่วยงานในสังกัดกรมอุทยานแห่งชาติ สัตว์ป่า และพันธุ์พืช และชำระเงินที่เคาน์เตอร์ธนาคารกรุงไทย หรือ ATM
- เว็บไซต์กรมศิลปากร เปิดจำหน่ายบัตรการแสดง และจำหน่ายหนังสือกรมศิลปากร โดยปัจจุบันรองรับการชำระเงินผ่านเลขที่อ้างอิง Bill Payment เท่านั้น
- เว็บไซต์ศูนย์มานุษยวิทยาสิรินธร เปิดจำหน่ายหนังสือ โดยสามารถชำระเงินผ่าน QR Payment, ชำระผ่านสาขาธนาคาร และโอนเงินผ่านหมายเลขบัญชีธนาคาร
- เว็บไซต์สำนักงานพัฒนาเทคโนโลยีอวกาศและภูมิสารสนเทศ เปิดจำหน่ายแผนที่และรูปภาพดาราศาสตร์ โดยสามารถชำระเงินผ่านบัตรเครดิต, โอนเงินผ่านธนาคาร, เก็บเงินปลายทางและชำระด้วยเงินสดเมื่อรับของที่ร้าน

จากข้อมูลข้างต้นแม้ว่าบางเว็บไซต์ของหน่วยงานรัฐ เว็บไซต์ที่ให้บริการซื้อขายสินค้า และเว็บไซต์ที่ให้บริการด้านการท่องเที่ยวและโรงแรมที่มีช่องทางการชำระเงินผ่านบัตรเครดิตแต่เว็บไซต์เหล่านี้ไม่ได้มีการเก็บหมายเลขบัตรเครดิตในระบบ เราจึงเปรียบเทียบนโยบายการกำหนดรหัสผ่านโดยอ้างอิงมาตรฐาน NIST

4.2 ผลการวิเคราะห์ความแข็งแรงของนโยบายรหัสผ่านของเว็บไซต์ในประเทศไทยเปรียบเทียบกับมาตรฐาน PCI DSS

จากตารางที่ 4.2 เมื่อเปรียบเทียบกับมาตรฐาน PCI DSS หัวข้อความยาวและจำนวนอักขระขั้นต่ำพบว่ามีเว็บไซต์ที่บังคับผู้ใช้งานกำหนดรหัสผ่านให้มีความยาวอย่างน้อย 7 ตัวอักษรโดยต้องประกอบด้วยตัวเลขและตัวอักษรภาษาอังกฤษ เพียง 9 จาก 16 เว็บไซต์คือ lazada.co.th, shopee.co.th, lotuss.com, central.co.th, airasia.com, tripadvisor.com, trip.com, klook.com และ emirates.com และเว็บไซต์ที่ไม่ได้ปฏิบัติตามมาตรฐานมีข้อบังคับการกำหนดนโยบายรหัสผ่านที่แตกต่างกันดังนี้

- บังคับให้ระบุความยาวรหัสผ่านอย่างน้อย 8 ตัวอักษรแต่สามารถระบุเพียงตัวเลขอย่างเดียวได้ คือ agoda.com และ traveloka

- บังคับให้ระบุความยาวรหัสผ่านอย่างน้อย 6 ตัวอักษรแต่สามารถระบุเพียงตัวเลขอย่างเดียวได้ คือ homepro.co.th และ thaiwatsadu.com
- เว็บไซต์บังคับให้ระบุความยาวรหัสผ่านอย่างน้อย 6 ตัวอักษร แต่ต้องประกอบด้วยตัวเลข ตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ ตัวอักษรภาษาอังกฤษพิมพ์เล็ก และอักขระพิเศษ !@$%*& คือ shopat24.com
- เว็บไซต์บังคับให้ระบุความยาวรหัสผ่านอย่างน้อย 6 ตัวอักษร แต่ต้องประกอบด้วยตัวเลข ตัวอักษรภาษาอังกฤษพิมพ์ใหญ่ ตัวอักษรภาษาอังกฤษพิมพ์เล็ก คือ bigc.co.th

เมื่อเปรียบเทียบกับมาตรฐาน PCI DSS หัวข้ออื่นคือห้ามใช้รหัสผ่านซ้ำกับรหัสผ่าน 4 ครั้งก่อนหน้า เราไม่สามารถหาข้อมูลของเว็บไซต์ bigc.co.th ได้เนื่องจากระบบไม่มีช่องทางการเปลี่ยนรหัสผ่าน นอกจากเว็บไซต์นี้ พบว่าเว็บไซต์ที่ห้ามใช้รหัสผ่านซ้ำกับรหัสผ่าน 4 ครั้งก่อนหน้าและห้ามใช้รหัสผ่านที่เคยพบว่ารั่วไหล มีเพียงเว็บไซต์เดียวที่ปฏิบัติตามนโยบายดังกล่าวคือ emirates.com แต่เว็บไซต์นี้ยินยอมให้รหัสผ่านที่เดาง่าย คือ BSword555

ผลการวิเคราะห์พบว่าไม่มีเว็บไซต์ใดใน 16 เว็บไซต์ปฏิบัติตามมาตรฐานในหัวข้อ
- ห้ามใช้รหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษร
- ห้ามใช้รหัสผ่านที่เดาง่าย

สำหรับมาตรฐาน PCI DSS หัวข้อต้องมีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด ในหัวข้อนี้หากเว็บไซต์มีการป้องกัน Brute Force Attack เช่นการ ใช้ captcha, การให้เลื่อนรูปภาพเพื่อยืนยันว่าเป็นบุคคลจะถือว่าเว็บไซต์มีการปฏิบัติตามนโยบายดังกล่าว โดยพบว่ามีเว็บไซต์ที่ปฏิบัติตามและไม่ปฏิบัติตามดังนี้
- เว็บไซต์ที่ปฏิบัติตามมี 11 เว็บไซต์คือ
    - lazada.co.th
    - shopee.co.th
    - homepro.co.th
    - thaiwatsadu.com
    - agoda.com
    - airasia.com
    - booking.com
    - trip.com
    - klook.com
    - traveloka.com
    - emirates.com

- เว็บไซต์ที่ไม่ปฏิบัติตามมี 5 เว็บไซต์คือ
    - shopat24.com
    - lotuss.com
    - central.co.th
    - bigc.co.th
    - tripadvisor.com

จากการศึกษาพบว่าเว็บไซต์ที่แสดงในตารางที่ 4.2 ผู้ใช้บริการสามารถเก็บบันทึกหมายเลขบัตรเครดิตในระบบแต่ทุกเว็บไซต์ ผู้ใช้งานไม่สามารถดูหมายเลขบัตรเครดิตแบบเต็ม 16 หลักได้ บางระบบแสดงเพียงสี่หลักสุดท้ายของหมายเลขบัตรเครดิต บางระบบแสดงเพียงหกหลักด้านหน้าและสี่หลักสุดท้ายของหมายเลขบัตรเครดิตเท่านั้น จากข้อมูลดังกล่าว จึงไม่สามารถทราบได้ว่าเว็บไซต์ที่เก็บข้อมูลบัตรเครดิตของผู้ใช้งานมีการรักษาความปลอดภัยข้อมูลส่วนนี้อย่างไร และระบบมีการบันทึกข้อมูลบัตรเครดิตทั้งหมดหรือไม่ ทั้งนี้เมื่อทำการชำระเงินแบบตัดบัตรเครดิตที่บันทึกไว้ บางระบบต้องระบุ Card Verification Value (CVV) หรือรหัสยืนยัน เพื่อดำเนินการทำธุรกรรมผ่านเว็บไซต์ แต่บางเว็บไซต์สามารถชำระเงินได้โดยไม่ต้องระบุ OTP ยืนยัน ซึ่งข้อกำหนดนี้ขึ้นอยู่กับธนาคารของผู้ถือบัตรเอง

สำหรับมาตรฐาน PCI DSS หัวข้อต้องใช้ MFA ในการเข้าสู่ระบบ พบว่ามีเพียง 2 เว็บไซต์ที่ปฏิบัติตามนโยบายดังกล่าวคือ lazada.com และ shopee.com ซึ่งเป็นเว็บไซต์ที่มียอดผู้เข้าใช้งานสูงสุดในหมวดหมู่ของเว็บไซต์ที่ให้บริการซื้อขายสินค้า และผู้ใช้บริการสามารถเก็บบัตรเครดิตในระบบเพื่อใช้ชำระเงินได้

4.3 แนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์แต่ละประเภทให้เป็นไปตามมาตรฐานของ สกมช., NIST และ PCI DSS

จากผลการศึกษาการวิเคราะห์ความแข็งแรงของนโยบายรหัสผ่านของเว็บไซต์ในประเทศไทย พบว่าบางเว็บไซต์มีการเก็บข้อมูลส่วนบุคคล บางเว็บไซต์เก็บทั้งข้อมูลหมายเลขบัตรเครดิตและข้อมูลส่วนบุคคล เราจึงขอเสนอแนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์แต่ละประเภทเพื่อให้เป็นไปตามมาตรฐาน ดังนี้

4.3.1 นโยบายในการกำหนดรหัสผ่านเว็บไซต์หน่วยงานรัฐ

เพื่อให้เป็นไปตามมาตรฐาน NIST เราขอเสนอให้เว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคลควรกำหนดนโยบายในการกำหนดรหัสผ่านดังนี้

- รหัสผ่านต้องมีความยาวอย่างน้อย 8 ตัวอักษร และไม่เกิน 64 ตัวอักษร
- ห้ามใช้รหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรม

- ห้ามใช้รหัสผ่านที่เคยพบว่ารั่วไหล
- มีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด หรือใช้ CAPCHA เพื่อป้องกัน Brute Force Attack
- ต้องใช้ Multi Factor Authentication

4.3.2 นโยบายในการกำหนดรหัสผ่านเว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคล

เพื่อให้เป็นไปตามมาตรฐาน NIST เราขอเสนอให้เว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคลควรกำหนดนโยบายในการกำหนดรหัสผ่านดังนี้

- รหัสผ่านต้องมีความยาวอย่างน้อย 8 ตัวอักษร
- ห้ามใช้รหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษร เช่น 12345, aaaaa
- ห้ามใช้รหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรม
- ห้ามใช้รหัสผ่านที่เคยพบว่ารั่วไหล
- มีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด
- ต้องใช้ MFA เมื่อมีการขอข้อมูลส่วนบุคคล

4.3.3 นโยบายในการกำหนดรหัสผ่านเว็บไซต์ที่มีการเก็บหมายเลขบัตรเครดิต

เพื่อให้เป็นไปตามมาตรฐาน PCI DSS เราขอเสนอให้เว็บไซต์ที่มีการเก็บข้อมูลบัตรเครดิตควรกำหนดนโยบายในการกำหนดรหัสผ่านดังนี้

- รหัสผ่านต้องมีความยาวอย่างน้อย 7 ตัวอักษร
- รหัสผ่านต้องประกอบด้วยตัวเลขและตัวอักษรภาษาอังกฤษ
- เปลี่ยนรหัสผ่านทุก 90 วัน และรหัสผ่านใหม่ต้องไม่ซ้ำกับรหัสผ่าน 4 ครั้งก่อนหน้า
- ห้ามใช้รหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรม
- ห้ามใช้รหัสผ่านที่เคยพบว่ารั่วไหล
- ต้องมีการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด
- ต้องใช้ MFA

4.4 แนวปฏิบัติที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่านสำหรับผู้พัฒนาระบบได้

จากผลการศึกษาเห็นได้อย่างชัดเจนว่าผู้พัฒนาเว็บไซต์ในประเทศไทยยังคงขาดความตระหนักรู้ด้านความปลอดภัย และมีนโยบายการกำหนดรหัสผ่านแตกต่างกันไป แม้ว่าหน่วยงานรัฐจะมีการกำหนดแนวทางแนะนำในการพัฒนาเว็บไซต์ให้ปลอดภัยจากสกมช. แต่หลายองค์กรไม่ได้นำมาบังคับใช้ และไม่มีหน่วยงานใดตรวจสอบเพื่อให้เป็นไปตามมาตรฐาน

เพื่อให้มั่นใจว่าผู้พัฒนาได้ปฏิบัติตามมาตรฐานอย่างถูกต้อง แนวทางปฏิบัตินี้จึงกำหนดวิธีการตรวจสอบการพัฒนาเว็บไซต์ว่าเป็นไปตามมาตรฐานหรือไม่โดยแบ่งเป็น 3 แนวปฏิบัติดังนี้

4.4.1 แนวปฏิบัติที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่านเว็บไซต์หน่วยงานรัฐ

เพื่อให้เป็นไปตามแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์เว็บไซต์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) งานวิจัยนี้จึงขอเสนอวิธีการตรวจสอบเว็บไซต์หน่วยงานรัฐว่าเป็นไปตามมาตรฐานหรือไม่ โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้

1) ระบุรหัสผ่านที่มีความยาวน้อยกว่า 8 ตัวอักษรและระบุรหัสผ่านที่มีความยาวมากกว่า 64 ตัวอักษร ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านดังกล่าว
2) ระบุรหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรมโดยใช้ชุดข้อมูล RockYou [11] ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว
3) ระบุรหัสผ่านที่เคยพบว่ารั่วไหลโดยใช้ชุดข้อมูล NCSC-HIBP-100k [13] ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว
4) ระบุรหัสผ่านที่ไม่ถูกต้อง 5 ครั้ง ระบบต้องให้ผู้ใช้บริการระบุ CAPCHA หรือระงับการเข้าใช้งานชั่วคราว หรือล็อคบัญชีผู้ใช้งาน
5) ระบุรหัสผ่านที่ใช้งานเพียงครั้งเดียว (One Time Password – OTP) ที่ไม่ถูกต้อง ระบบต้องไม่อนุญาตให้เข้าใช้งาน

4.4.2 แนวปฏิบัติที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่านเว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคล

หลังจากที่มีการบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act) เพื่อให้องค์กรต่าง ๆ ที่มีการประมวลผลข้อมูลส่วนบุคคล ควรให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล และพัฒนาระบบที่เกี่ยวข้องอย่างปลอดภัยและเป็นไปตามมาตรฐานสากล ซึ่งปัจจุบันยังไม่มีหน่วยงานใดกำหนดข้อบังคับที่ชัดเจน รวมถึงวิธีการตรวจสอบว่าปฏิบัติตามมาตรฐานหรือไม่ งานวิจัยนี้จึงเสนอวิธีการตรวจสอบเว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคลว่าเป็นไปตามมาตรฐาน NIST หรือไม่ โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้

โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้

1) ระบุรหัสผ่านที่มีความยาวน้อยกว่า 8 ตัวอักษรและระบุรหัสผ่านที่มีความยาวมากกว่า 64 ตัวอักษร ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านดังกล่าว

2) ระบุรหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษรโดยใช้ชุดข้อมูล sequencePwd [14] ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่มีส่วนประกอบของรหัสผ่านตรงกับชุดข้อมูลดังกล่าว
3) ระบุรหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรมโดยใช้ชุดข้อมูล RockYou [11] ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว
4) ระบุรหัสผ่านที่เคยพบว่ารั่วไหลโดยใช้ชุดข้อมูล NCSC-HIBP-100k [13] ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว
5) ระบุรหัสผ่านที่ไม่ถูกต้อง 5 ครั้ง ระบบต้องให้ผู้ใช้บริการระบุ CAPCHA หรือระงับการเข้าใช้งานชั่วคราว หรือล็อคบัญชีผู้ใช้งาน
6) ระบุรหัสผ่านที่ใช้งานเพียงครั้งเดียว (One Time Password – OTP) ที่ไม่ถูกต้อง ระบบต้องไม่อนุญาตให้เข้าใช้งาน

4.4.3 แนวปฏิบัติที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่านเว็บไซต์ที่มีการเก็บข้อมูลบัตรเครดิต

ปัจจุบันการซื้อสินค้าและบริการผ่านเว็บไซต์เติบโตขึ้นมากในประเทศไทย บางระบบเสนอช่องทางการชำระเงินให้ผู้ใช้บริการสามารถเลือกใช้ได้ตามความสะดวก และยังสามารถเก็บข้อมูลการชำระเงินในระบบเพื่อใช้ในครั้งถัดไปได้ กรณีผู้ใช้งานเลือกชำระเงินผ่านช่องทางบัตรเครดิตและเก็บข้อมูลบัตรลงในระบบ จะมั่นใจได้อย่างไรว่าระบบมีความปลอดภัย เพื่อให้ผู้พัฒนาได้ตรวจสอบความปลอดภัยของระบบตนเองว่าได้พัฒนาส่วนของนโยบายการกำหนดรหัสผ่านตามมาตรฐานสากล งานวิจัยนี้จึงเสนอวิธีการตรวจสอบเว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคลว่าเป็นไปตามมาตรฐาน PCI DSS หรือไม่ โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้

โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้

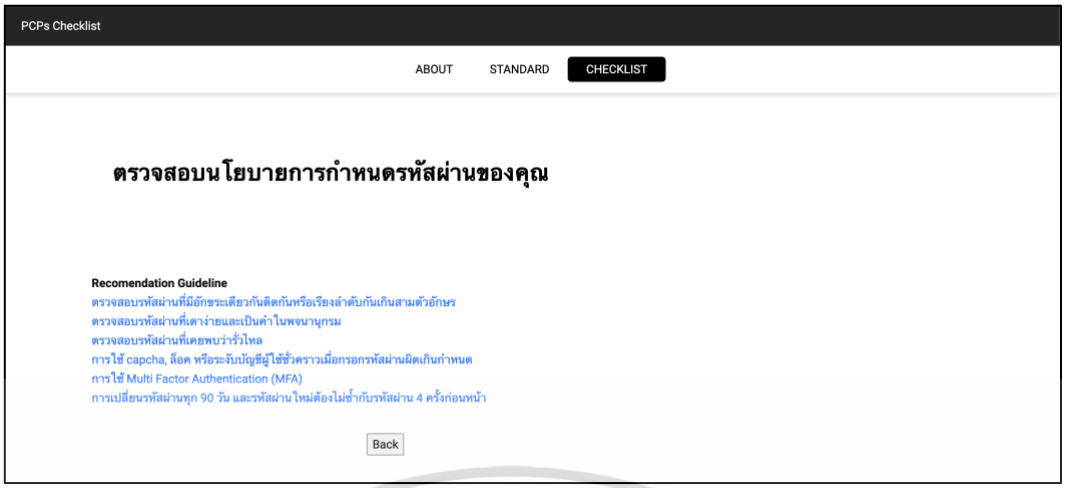
1) ระบุรหัสผ่านที่มีความยาวน้อยกว่า 7 ตัวอักษรและต้องประกอบด้วยตัวเลขและตัวอักษรอย่างน้อยหนึ่งตัว หากไม่ตรงตามข้อกำหนด ระบบต้องไม่อนุญาตให้ใช้รหัสผ่านดังกล่าว
2) ระบุรหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษรโดยใช้ชุดข้อมูล sequencePwd [14] ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่มีส่วนประกอบของรหัสผ่านตรงกับชุดข้อมูลดังกล่าว
3) ระบุรหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรมโดยใช้ชุดข้อมูล RockYou [11] ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว
4) ระบุรหัสผ่านที่เคยพบว่ารั่วไหลโดยใช้ชุดข้อมูล NCSC-HIBP-100k [13] ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว
5) ระบุรหัสผ่านที่ไม่ถูกต้อง 5 ครั้ง ระบบต้องให้ผู้ใช้บริการระบุ CAPCHA หรือระงับการเข้าใช้งานชั่วคราว หรือล็อคบัญชีผู้ใช้งาน

6) เข้าสู่เมนูเปลี่ยนรหัสผ่าน และทำการเปลี่ยนรหัสโดยใช้รหัสเดิมระบบต้องไม่อนุญาตให้ใช้รหัสผ่านดังกล่าว
7) เข้าสู่เมนูเปลี่ยนรหัสผ่าน และทำการเปลี่ยนรหัสโดยใช้รหัส 4 ครั้ง และทำการเปลี่ยนรหัสผ่านอีกครั้งโดยระบุรหัสผ่านที่กำหนดครั้งแรก ระบบต้องไม่อนุญาตให้ใช้รหัสผ่านดังกล่าว
8) ระบุรหัสผ่านที่ใช้งานเพียงครั้งเดียว (One Time Password – OTP) ที่ไม่ถูกต้อง ระบบต้องไม่อนุญาตให้เข้าใช้งาน

4.4.4 เครื่องมือที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่านเว็บไซต์

เพื่อให้ผู้พัฒนาเว็บไซต์สามารถตรวจสอบนโยบายในการกำหนดรหัสผ่านเว็บไซต์ของตนว่าได้ปฏิบัติตามคำแนะนำตามมาตรฐานหรือไม่ ผู้วิจัยได้พัฒนาเครื่องมือสำหรับตรวจสอบนโยบายในการกำหนดรหัสผ่านเว็บไซต์โดยอ้างอิงตามมาตรฐาน สกมช, NIST และ PCI DSS รวมถึงให้คำแนะนำหากไม่ได้ปฏิบัติตามในแต่ละหัวข้อ ดังแสดงในรูปที่ 4.1 และ 4.2

รูปที่ 4.1 ตัวอย่างหน้าจอตรวจสอบนโยบายการกำหนดรหัสผ่าน



รูปที่ 4.2 ตัวอย่างหน้าจอคำแนะนำการพัฒนานโยบายการกำหนดรหัสผ่าน

จากรูปที่ 4.1 ผู้พัฒนาสามารถตรวจสอบนโยบายการกำหนดรหัสผ่านเว็บไซต์ที่พัฒนาว่าได้ปฏิบัติตามคำแนะนำตามมาตรฐานหรือไม่ ในกรณีที่ไม่ได้ปฏิบัติตามในหัวข้อใด เมื่อกดปุ่ม Check PCPs เครื่องมือจะให้คำแนะนำในแต่ละหัวข้อ ซึ่งผู้พัฒนาสามารถเรียกดูวิธีการพัฒนา รวมถึงดาวน์โหลดชุดข้อมูลสำหรับใช้ตรวจสอบและพัฒนาได้จากหน้าจอตามรูปที่ 4.2

4.5 ผลสำรวจระดับความยากง่ายและความเต็มใจของผู้ใช้บริการในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านตามมาตรฐาน

งานวิจัยนี้ทำการสอบถามผู้ใช้บริการเว็บไซต์ จำนวน 62 คน โดยแบ่งเป็น

- เพศ
  - หญิง จำนวน 36 คน
  - เพศชาย จำนวน 26 คน
- อายุ
  - 20 - 30 ปี จำนวน 36 คน
  - 30 – 40 ปี จำนวน 20 คน
  - มากกว่า 40 ปี จำนวน 6 คน
- อาชีพ
  - พนักงานบริษัทด้าน IT จำนวน 16 คน
  - พนักงานบริษัทที่ไม่เกี่ยวข้องกับ IT จำนวน 30 คน
  - ธุรกิจส่วนตัว/อื่นๆ จำนวน 16 คน

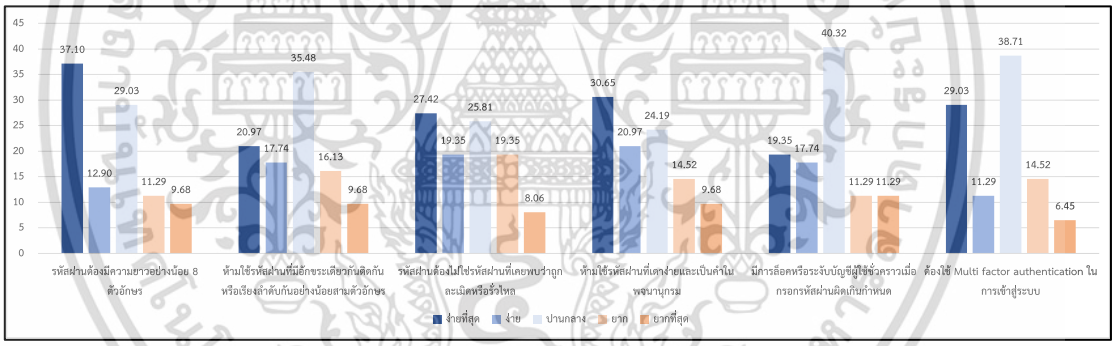
การสำรวจระดับความยากง่ายในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านแต่ละหัวข้อ แบ่งออกเป็น 5 ระดับคือ ง่ายที่สุด ง่าย ปานกลาง ยาก และยากที่สุด

การสำรวจระดับความเต็มใจในการปฏิบัติตามนโยบายทุกข้อ แบ่งออกเป็น 5 ระดับ คือ

- เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง
- เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง
- ไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์
- ไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง
- ไม่เต็มใจเลยและไม่ปฏิบัติตามเนื่องจากยอมรับความเสี่ยงได้

4.5.1 ผลสำรวจตามมาตรฐานของ NIST

ผลการสำรวจพบว่าผู้ใช้บริการสามารถปฏิบัติตามนโยบายในแต่ละหัวข้อ ไม่มีนโยบายใดที่ผู้ใช้บริการปฏิบัติได้ยาก หรือยากที่สุดมากกว่าร้อยละ 20 มากกว่า และพบว่าสามารถปฏิบัติตามได้ง่ายที่สุดในทุกนโยบาย ยกเว้นการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผิดเกินกำหนด โดยหัวข้อดังกล่าวผู้ใช้ส่วนใหญ่สามารถปฏิบัติตามได้ในระดับปานกลาง และ ดังแสดงในรูปที่ 4.1



รูปที่ 4.3 ระดับความยากง่ายในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST

ผลการสำรวจในหัวข้อรหัสผ่านต้องยาวขั้นต่ำ 8 ตัวอักษร ผู้ใช้บริการสามารถปฏิบัติตามได้ง่ายที่สุดถึงร้อยละ 37.1 ปฏิบัติตามได้ง่ายร้อยละ 12.9 ปฏิบัติตามได้ปานกลางร้อยละ 29.03 ปฏิบัติตามได้ยากร้อยละ 11.29 และปฏิบัติตามได้ยากที่สุดร้อยละ 9.68 จากรูปที่ 4.3 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับง่ายที่สุด

ผลการสำรวจในหัวข้อห้ามใช้รหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษร ผู้ใช้บริการร้อยละ 35.48 สามารถปฏิบัติตามได้ในระดับปานกลาง รองลงมาคือระดับง่ายที่สุด ง่าย ยาก ยากที่สุด โดยคิดเป็นร้อยละ 20.97, 17.74, 16.13 และ 9.68 ตามลำดับ จากรูปที่ 4.3 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับปานกลาง

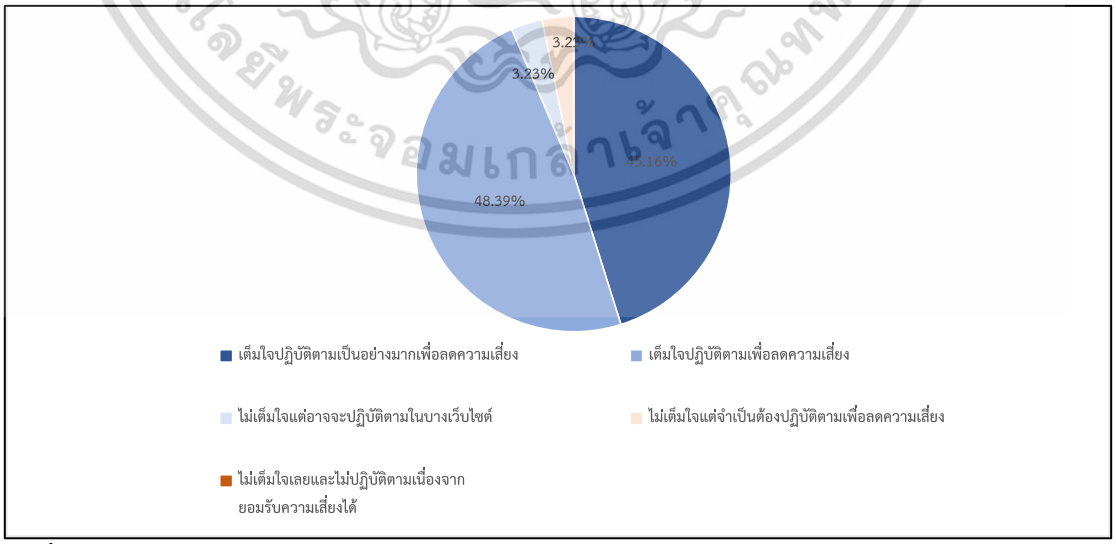
ผลการสำรวจในหัวข้อรหัสผ่านต้องไม่ใช่รหัสผ่านที่เคยพบว่าถูกละเมิดหรือรั่วไหล ผู้ใช้บริการสามารถปฏิบัติตามได้ง่ายที่สุดร้อยละ 27.42 ปฏิบัติตามได้ง่ายร้อยละ 19.35 ปฏิบัติตามได้ปานกลางร้อยละ 25.81 ปฏิบัติตามได้ยากร้อยละ 19.35 และปฏิบัติตามได้ยากที่สุดร้อยละ 8.06 จากรูปที่ 4.3 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับง่ายที่สุด

ผลการสำรวจในหัวข้อห้ามใช้รหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรม ผู้ใช้บริการสามารถปฏิบัติตามได้ง่ายที่สุดร้อยละ 30.65 ปฏิบัติตามได้ง่ายร้อยละ 20.97 ปฏิบัติตามได้ปานกลางร้อยละ 24.19 ปฏิบัติตามได้ยากร้อยละ 14.52 และปฏิบัติตามได้ยากที่สุดร้อยละ 9.68 จากรูปที่ 4.3 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับง่ายที่สุด

ผลการสำรวจในหัวข้อการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด ผู้ใช้บริการร้อยละ 40.32 สามารถปฏิบัติตามได้ในระดับปานกลาง รองลงมาคือระดับง่ายที่สุดร้อยละ 19.35 ปฏิบัติตามได้ง่ายร้อยละ 17.74 ปฏิบัติตามได้ยากและยากที่สุดร้อยละ 11.29 จากรูปที่ 4.3 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับปานกลาง

ผลการสำรวจในหัวข้อต้องใช้ MFA ในการเข้าสู่ระบบ ผู้ใช้บริการร้อยละ 38.71 สามารถปฏิบัติตามได้ในระดับปานกลาง รองลงมาคือระดับง่ายที่สุดร้อยละ 29.03 ลำดับถัดมาคือยากร้อยละ 14.52 ง่ายร้อยละ 11.29 และยากที่สุดร้อยละ 6.45 จากรูปที่ 4.3 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับปานกลาง

จากผลสำรวจข้างต้นผู้ใช้บริการส่วนใหญ่สามารถปฏิบัติตามได้ในระดับปานกลางถึงง่ายที่สุด ซึ่งนอกจากประเด็นความยากง่ายในการปฏิบัติตามแล้ว เมื่อสำรวจด้านความเต็มใจในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST ทุกนโยบายที่เสนอแนะในงานวิจัยนี้ กลับพบว่าแม้จะไม่สามารถปฏิบัติตามได้ง่ายที่สุดในทุกนโยบาย แต่มากกว่าร้อยละ 90 มีความเต็มใจในการปฏิบัติตาม โดยผลการสำรวจแสดงดังรูปที่ 4.4



รูปที่ 4.4 ระดับความเต็มใจของผู้ใช้บริการในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST

จากรูปที่ 4.4 แสดงให้เห็นถึงระดับความเต็มใจของผู้ใช้บริการหากเว็บไซต์ที่เก็บข้อมูลส่วนบุคคลมีการบังคับนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST โดยร้อยละ 45.16 เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง ร้อยละ 48.39 เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง และร้อยละ 3.23 ไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง

ข้อมูลจากแบบสอบถามเมื่อแบ่งตามเพศของผู้ใช้บริการพบว่า

- เพศหญิงจำนวน 36 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 17 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 16 คน ไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์ 1 คน และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง 2 คน
- เพศชายจำนวน 26 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 11 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 14 คน และไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์ 1 คน

ข้อมูลจากแบบสอบถามเมื่อแบ่งตามอายุของผู้ใช้บริการพบว่า

- อายุ 20 - 30 ปี จำนวน 36 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 17 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 17 คน ไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์ 1 คน และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง 1 คน
- อายุ 30 – 40 ปี จำนวน 20 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 8 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 11 คน และไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์ 1 คน
- อายุมากกว่า 40 ปี จำนวน 6 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 3 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 2 คน และไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์ 1 คน

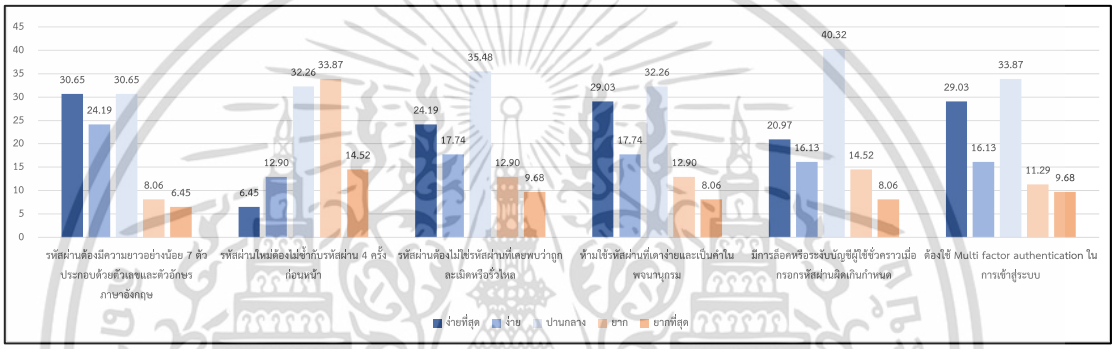
ข้อมูลจากแบบสอบถามเมื่อแบ่งตามอาชีพของผู้ใช้บริการพบว่า

- พนักงานบริษัทด้าน IT จำนวน 16 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 8 คน และเต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 8 คน โดยไม่มีท่านใดระบุว่าไม่เต็มใจปฏิบัติตาม
- พนักงานบริษัทที่ไม่เกี่ยวข้องกับ IT จำนวน 30 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 13 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 15 คน ไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์ 1 คน และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง 1 คน
- ธุรกิจส่วนตัว/อื่นๆ จำนวน 16 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 7 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 7 คน ไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์ 1 คน และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง 1 คน

จากข้อมูลข้างต้นสรุปได้ว่าผู้ใช้บริการไม่ว่าเพศใด อายุเท่าใด และทำงานด้าน IT หรือไม่ ส่วนใหญ่มีความเต็มใจปฏิบัติตามนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST และไม่มีผู้ใช้บริการระบุว่าไม่เต็มใจเลยและไม่ปฏิบัติตามเนื่องจากยอมรับความเสี่ยงได้

4.5.2 ผลสำรวจตามมาตรฐานของ PCI DSS

ผลการสำรวจพบว่าผู้ใช้บริการสามารถปฏิบัติตามนโยบายในแต่ละหัวข้อ พบว่าการเปลี่ยนรหัสผ่านทุก 90 วัน และต้องไม่ซ้ำกับรหัสผ่าน 4 ครั้งที่เคยใช้งานก่อนหน้าสามารถปฏิบัติตามได้ยากถึงร้อยละ 33.87 ในขณะที่หัวข้ออื่นสามารถปฏิบัติตามได้ง่ายที่สุดเกินร้อยละ 20 และผู้ใช้งานส่วนใหญ่สามารถปฏิบัติตามในระดับปานกลาง ดังแสดงในรูปที่ 4.5



รูปที่ 4.5 ระดับความยากง่ายในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ PCI DSS

ผลการสำรวจในหัวข้อรหัสรหัสผ่านต้องมีความยาวอย่างน้อย 7 ตัวประกอบด้วยตัวเลขและตัวอักษรภาษาอังกฤษ ผู้ใช้บริการสามารถปฏิบัติตามได้ง่ายที่สุดและปานกลางร้อยละ 30.65 สามารถปฏิบัติตามได้ง่ายร้อยละ 24.19 ปฏิบัติตามได้ยากร้อยละ 8.06 และปฏิบัติตามได้ยากที่สุดร้อยละ 6.45 จากรูปที่ 4.5 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับง่ายที่สุด

ผลการสำรวจในหัวข้อการเปลี่ยนรหัสผ่านทุก 90 วัน และต้องไม่ซ้ำกับรหัสผ่าน 4 ครั้งที่เคยใช้งานก่อนหน้าสามารถปฏิบัติตามได้ยากถึงร้อยละ 33.87 รองลงมายังคงปฏิบัติตามได้ในระดับปานกลางร้อยละ 32.26 ปฏิบัติตามได้ยากที่สุดร้อยละ 14.52 ปฏิบัติตามได้ง่ายร้อยละ 12.90 และปฏิบัติตามได้ง่ายที่สุดเพียงร้อยละ 6.45 จากรูปที่ 4.5 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับยาก

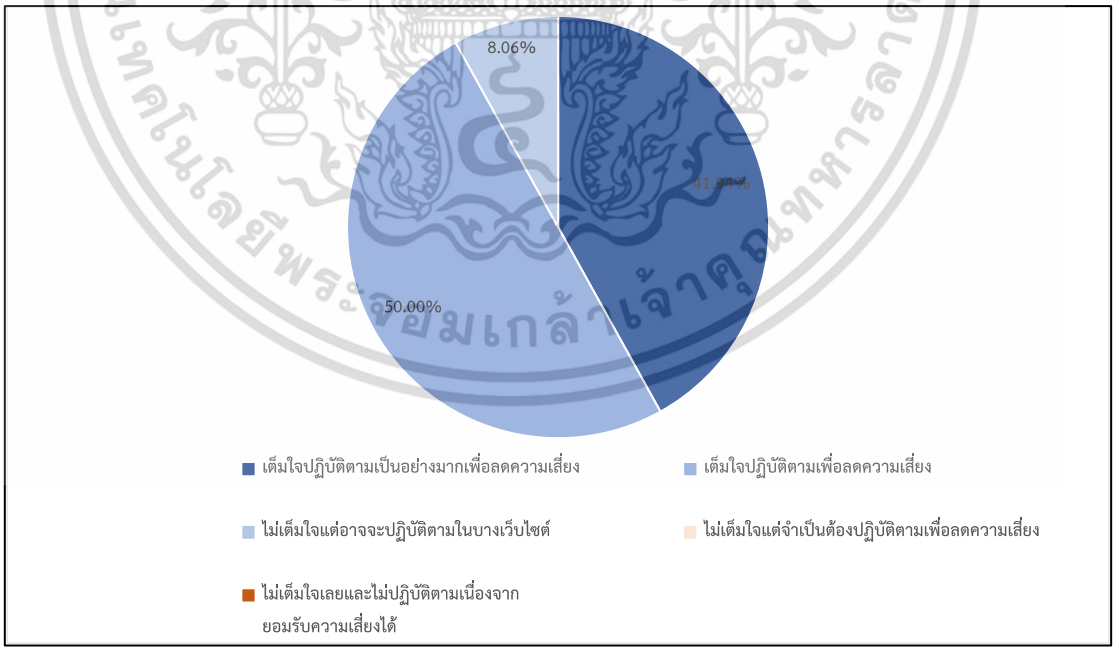
ผลการสำรวจในหัวข้อรหัสผ่านต้องไม่ใช่รหัสผ่านที่เคยพบว่าถูกละเมิดหรือรั่วไหล ผู้ใช้บริการร้อยละ 35.48 สามารถปฏิบัติตามได้ในระดับปานกลาง รองลงมาคือระดับง่ายที่สุด ง่าย ยาก ยากที่สุด โดยคิดเป็นร้อยละ 24.19, 17.74, 12.90 และ 9.68 ตามลำดับ จากรูปที่ 4.1 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับปานกลาง

ผลการสำรวจในหัวข้อห้ามใช้รหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรม ผู้ใช้บริการร้อยละ 32.26 สามารถปฏิบัติตามได้ในระดับปานกลาง รองลงมาคือระดับง่ายที่สุด ง่าย ยาก ยากที่สุด โดยคิดเป็นร้อยละ 29.03, 17.74, 12.90 และ 8.06 ตามลำดับ จากรูปที่ 4.5 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับปานกลาง

ผลการสำรวจในหัวข้อการล็อคหรือระงับบัญชีผู้ใช้ชั่วคราวเมื่อกรอกรหัสผ่านผิดเกินกำหนด ผู้ใช้บริการร้อยละ 40.32 สามารถปฏิบัติตามได้ในระดับปานกลาง รองลงมาคือระดับง่ายที่สุด ง่าย ยาก ยากที่สุด โดยคิดเป็นร้อยละ 20.97, 16.13, 14.52 และ 8.06 ตามลำดับ จากรูปที่ 4.5 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับปานกลาง

ผลการสำรวจในหัวข้อต้องใช้ Multi factor authentication ในการเข้าสู่ระบบผู้ใช้บริการ ร้อยละ 33.87 สามารถปฏิบัติตามได้ในระดับปานกลาง รองลงมาคือระดับง่ายที่สุด ง่าย ยาก ยากที่สุด โดยคิดเป็นร้อยละ 29.03, 16.13, 11.29 และ 9.68 ตามลำดับ จากรูปที่ 4.5 สรุปได้ว่านโยบายนี้สามารถปฏิบัติตามได้ในระดับปานกลาง

จากผลสำรวจข้างต้นผู้ใช้บริการส่วนใหญ่สามารถปฏิบัติตามได้ในระดับปานกลาง ซึ่งถึงแม้ว่าบางหัวข้อจะปฏิบัติตามได้ยาก เมื่อสำรวจด้านความเต็มใจในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ PCI DSS ทุกนโยบายที่เสนอแนะในงานวิจัยนี้ กลับพบว่าผู้ใช้บริการส่วนใหญ่มากกว่าร้อยละ 90 มีความเต็มใจในการปฏิบัติตาม โดยผลการสำรวจแสดงดังรูปที่ 4.6



รูปที่ 4.6 ระดับความเต็มใจของผู้ใช้บริการในการปฏิบัติตามข้อตกลงและนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ PCI DSS

จากรูปที่ 4.6 แสดงให้เห็นถึงระดับความเต็มใจของผู้ใช้บริการหากเว็บไซต์ที่เก็บหมายเลขบัตรเครดิตในระบบมีการบังคับนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ PCI DSS ผลสำรวจพบว่า ร้อยละ 50 เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง ร้อยละ 41.94 เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง และร้อยละ 8.06 ไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์ โดยเมื่อแยกผลสำรวจตามเพศ อายุ และอาชีพ ได้ข้อมูลดังนี้

ข้อมูลจากแบบสอบถามเมื่อแบ่งตามเพศของผู้ใช้บริการพบว่า

- เพศหญิงจำนวน 36 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 16 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 16 คน และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง 4 คน
- เพศชายจำนวน 26 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 10 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 15 คน และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง 1 คน

ข้อมูลจากแบบสอบถามเมื่อแบ่งตามอายุของผู้ใช้บริการพบว่า

- อายุ 20 - 30 ปี จำนวน 36 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 17 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 17 คน และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง 2 คน
- อายุ 30 – 40 ปี จำนวน 20 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 7 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 12 คน และไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์ 1 คน
- อายุมากกว่า 40 ปี จำนวน 6 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง และไม่เต็มใจแต่อาจจะปฏิบัติตามในบางเว็บไซต์อย่างละ 2 คน

ข้อมูลจากแบบสอบถามเมื่อแบ่งตามอาชีพของผู้ใช้บริการพบว่า

- พนักงานบริษัทด้าน IT จำนวน 16 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 7 คน และเต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 9 คน โดยไม่มีท่านใดระบุว่าไม่เต็มใจปฏิบัติตาม
- พนักงานบริษัทที่ไม่เกี่ยวข้องกับ IT จำนวน 30 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 12 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 16 คน และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามในบางเว็บไซต์ 2 คน
- ธุรกิจส่วนตัว/อื่นๆ จำนวน 16 คน เต็มใจปฏิบัติตามเป็นอย่างมากเพื่อลดความเสี่ยง 7 คน เต็มใจปฏิบัติตามเพื่อลดความเสี่ยง 6 คน และไม่เต็มใจแต่จำเป็นต้องปฏิบัติตามเพื่อลดความเสี่ยง 3 คน

จากข้อมูลข้างต้นสรุปได้ว่าผู้ใช้บริการไม่ว่าเพศใด อายุเท่าใด และทำงานด้าน IT หรือไม่ ส่วนใหญ่มีความเต็มใจปฏิบัติตามนโยบายการกำหนดรหัสผ่านตามมาตรฐานของ NIST และไม่มีผู้ใช้บริการระบุว่าไม่เต็มใจเลยและไม่ปฏิบัติตามเนื่องจากยอมรับความเสี่ยงได้

4.6 ผลประเมินนโยบายการกำหนดรหัสผ่านจากผู้เชี่ยวชาญและผู้พัฒนาระบบ

เพื่อเป็นการประเมินแนวปฏิบัติสำหรับตรวจสอบนโยบายการกำหนดรหัสผ่านเว็บไซต์ งานวิจัยนี้ทำการสอบถามผู้เชี่ยวชาญถึงแนวทางที่นำเสนอว่าเห็นด้วยหรือไม่ และมีคำแนะนำเพิ่มเติมด้านใดบ้าง รวมถึงสอบถามไปยังนักพัฒนาเว็บไซต์ขององค์กรต่างๆ ถึงแนวปฏิบัติและนโยบายที่นำเสนอสร้างความตระหนักรู้ให้กับนักพัฒนาหรือไม่

4.6.1 ผลประเมินนโยบายการกำหนดรหัสผ่านจากผู้เชี่ยวชาญ

จากข้อเสนอแนะแนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์แต่ละประเภทให้เป็นไปตามมาตรฐานของ สกมช., NIST และ PCI DSS ดังที่กล่าวถึงในหัวข้อ 4.3 ผู้วิจัยได้จัดทำแนวปฏิบัติสำหรับตรวจสอบนโยบายการกำหนดรหัสผ่านเว็บไซต์ และสอบถามผู้เชี่ยวชาญด้านการพัฒนาเว็บไซต์ให้มีความปลอดภัย เพื่อประเมินแนวปฏิบัติดังกล่าว โดยได้รับการประเมินจากผู้เชี่ยวชาญจำนวน 5 ท่าน ซึ่งเป็นผู้เชี่ยวชาญที่ได้รับการรับรอง Cyber Security Foundation Professional Certificate – CSFPC และผู้พัฒนาเว็บไซต์ตำแหน่ง Product Leader ผลการประเมินคือเห็นด้วยกับข้อเสนอแนะดังกล่าว แต่มีความเห็นเพิ่มเติมว่าเป็นเรื่องยากที่จะบังคับให้ผู้ใช้บริการปฏิบัติตามนโยบายทุกข้อ โดยเฉพาะการต้องเปลี่ยนรหัสผ่านบ่อยๆ แต่หากผู้ใช้งานมีความตระหนักรู้ในด้านความปลอดภัยแล้วอาจยินดีที่จะปฏิบัตินโยบายดังที่เสนอมาได้ ซึ่งคำแนะนำดังกล่าวสอดคล้องกับผลสำรวจความเต็มใจในการปฏิบัติตามนโยบายการกำหนดรหัสผ่านดังที่ได้แสดงในหัวข้อ4.5 ทั้งนี้ผู้ให้บริการเว็บไซต์เองควรตระหนักถึงการรักษาความปลอดภัยของข้อมูลที่จัดเก็บในระบบด้วย หากไม่สามารถกำหนดข้อบังคับด้านรหัสผ่านของผู้ใช้งานได้ทุกข้อตามมาตรฐาน ก็ควรต้องมีมาตรการป้องกันอื่นเพื่อรักษาความปลอดภัยให้ระบบและรักษาความปลอดภัยแก่ข้อมูลของผู้ใช้บริการ ยกตัวอย่างเช่นการ scan ความปลอดภัยของ server อยู่เป็นประจำ การกำหนดสิทธิ์การเข้าถึงข้อมูลในระบบ เป็นต้น

4.6.2 ผลประเมินนโยบายการกำหนดรหัสผ่านจากผู้พัฒนาระบบ

จากข้อเสนอแนะแนวทางการกำหนดนโยบายในการกำหนดรหัสผ่านเว็บไซต์แต่ละประเภทให้เป็นไปตามมาตรฐานของ สกมช., NIST และ PCI DSS ดังที่กล่าวถึงในหัวข้อ 4.4.4 ผู้วิจัยได้จัดทำแนวปฏิบัติสำหรับตรวจสอบนโยบายการกำหนดรหัสผ่านเว็บไซต์ และสอบถามผู้พัฒนาระบบว่าเครื่องมือดังกล่าวช่วยสร้างความตระหนักรู้ให้กับนักพัฒนาในด้านนโยบายการกำหนดรหัสผ่านเว็บไซต์หรือไม่ นักพัฒนาเว็บไซต์ขององค์กรที่มีกรอบบังคับชัดเจน เช่นธนาคาร หรือบริษัท vendor ของธนาคาร ส่วนใหญ่มีความตระหนักรู้ในนโยบายการกำหนดรหัสผ่านดังกล่าว และมีการพัฒนาระบบในส่วนนี้ตามมาตรฐานแล้ว แต่นักพัฒนาเว็บไซต์องค์กรอื่นๆ มีการกำหนดนโยบายการกำหนดรหัสผ่านแตกต่างกันไปซึ่งไม่ได้ปฏิบัติตามมาตรฐานในบางหัวข้อ นโยบายด้านความยาวและความซับซ้อนของรหัสผ่านก็มีการพัฒนาที่แตกต่างกันไป โดยไม่ได้คำนึงถึงประเภทข้อมูลที่จัดเก็บ

เนื่องจากองค์กรไม่มีกรอบบังคับที่ชัดเจนและไม่ได้มีการตรวจสอบระบบอย่างเคร่งครัด รวมถึงนักพัฒนาระบบเองไม่ได้มีความตระหนักรู้ในส่วนนี้ จึงไม่ได้พัฒนาตามมาตรฐาน และมองว่าเครื่องมือนี้เป็นประโยชน์กับนักพัฒนาระบบที่สามารถนำมาใช้เป็นแนวทางในการพัฒนาและตรวจสอบระบบของตนได้

บทที่ 5

สรุปผลการวิจัยและข้อเสนอแนะ

จากการศึกษาวิเคราะห์งานวิจัยนี้พบว่าเว็บไซต์ของหน่วยงานต่างๆ ในประเทศไทยมีนโยบายการกำหนดรหัสผ่านในด้านความยาวและความซับซ้อนของรหัสผ่านเพียง 22 เว็บไซต์จากทั้งหมด 40 เว็บไซต์ในกลุ่มตัวอย่างของงานวิจัยนี้ สำหรับนโยบายด้านอื่นๆ เช่น ห้ามใช้รหัสผ่านที่เดาง่าย ห้ามใช้รหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันอย่างน้อยสามตัวอักษร ไม่มีเว็บไซต์ใดเลยที่ปฏิบัติตามคำแนะนำดังกล่าว รหัสผ่านที่พบบ่อยเช่น 12345678, Password, Password123 ระบบยังคงยินยอมให้กำหนดรหัสผ่านได้ เห็นได้ชัดว่าผู้พัฒนาไม่ได้มีความตระหนักรู้ในด้านการพัฒนาเว็บไซต์ให้ปลอดภัยในส่วนของนโยบายการกำหนดรหัสผ่าน และไม่มีหน่วยงานหรือองค์กรใดตรวจสอบความปลอดภัยเว็บไซต์ดังกล่าว แม้จะมียอดผู้ใช้งานค่อนข้างสูง และมีแนวโน้มเติบโตขึ้นอีกก็ตาม อย่างไรก็ดี งานวิจัยนี้ได้นำเสนอวิธีการตรวจสอบนโยบายการกำหนดรหัสผ่านเว็บไซต์โดยอ้างอิงตามมาตรฐานที่บังคับใช้ในหน่วยงานรัฐไทย และอ้างอิงตามมาตรฐานมาตรฐานสากลดังรายละเอียดที่ระบุในบทก่อนหน้า เพื่อให้ผู้พัฒนาได้นำไปใช้ตรวจสอบระบบให้มีความปลอดภัยยิ่งขึ้น เพื่อเพิ่มความเชื่อมั่นให้กับผู้ใช้บริการ และผู้ใช้งานยังคงเต็มใจปฏิบัติตามนโยบายการกำหนดรหัสผ่านดังกล่าว เพื่อเป็นการรักษาความปลอดภัยข้อมูลของตน

5.1 ข้อเสนอแนะ

เนื่องจากงานวิจัยนี้ทำการศึกษาเฉพาะกลุ่มตัวอย่างเว็บไซต์เพียง 3 กลุ่มคือเว็บไซต์หน่วยงานรัฐ เว็บไซต์ที่ให้บริการซื้อขายสินค้าและเว็บไซต์ที่ให้บริการด้านการท่องเที่ยวและโรงแรม อีกทั้งยังศึกษาบนระบบเว็บแอพพลิเคชันเท่านั้น ซึ่งปัจจุบันผู้ใช้บริการส่วนใหญ่ใช้งานผ่านแอพพลิเคชันบนมือถือเพิ่มมากขึ้น การขยายผลการวิเคราะห์นโยบายการกำหนดรหัสผ่านบนแอพพลิเคชันมือถือในประเทศไทย และเสนอแนวทางที่เหมาะสมกับแอพพลิเคชันแต่ละประเภท จึงเป็นอีกหนึ่งงานวิจัยที่น่าสนใจ และน่าจะเกิดประโยชน์กับประเทศมากยิ่งขึ้น

เครื่องมือที่ใช้ในการตรวจสอบความปลอดภัยของนโยบายในการกำหนดรหัสผ่านเว็บไซต์ที่พัฒนาในงานวิจัยนี้ได้รับการประเมินจากผู้พัฒนาระบบจากบางองค์กรเท่านั้น จึงไม่มีผลการประเมินเชิงประจักษ์ว่าได้สร้างความตระหนักรู้ให้กับนักพัฒนาเว็บไซต์ สำหรับงานวิจัยถัดไปควรมีการประเมินส่วนนี้เพิ่มเติม เพื่อตรวจสอบว่านักพัฒนาเว็บไซต์มีความตระหนักรู้ด้านนโยบายการกำหนดรหัสผ่านเพิ่มขึ้นหลังจากใช้เครื่องมือดังกล่าว

เอกสารอ้างอิง

[1] ธนาคารไทยพาณิชย์. 2023. **PDPA พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล เรื่องใกล้ตัวที่ทุกคนต้องรู้.** [Online]. Available : https://www.scb.co.th/th/personal-banking/stories/tips-for-you/pdpa-about-us.html

[2] ธนาคารแห่งประเทศไทย. 2023. **EC_EI_028_S2 เครื่องชี้ภาวะการท่องเที่ยว.** [Online]. Available: https://app.bot.or.th/BTWS_STAT/statistics/BOTWEBSTAT.aspx?reportID=875&language=TH

[3] สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. **มาตรฐานและแนวปฏิบัติ** [Online] Available: https://www.ncsa.or.th/standards-and-practices.html

[4] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. 2021. **ETDA เผยมูลค่าอีคอมเมิร์ซไทย ปี 63 อยู่ที่ 3.78 ล้านล้านบาท คาดปี 64 พุ่งไปที่ 4.01 ล้านล้านบาท.** [Online]. Available: https://www.etda.or.th/th/pr-news/ETDA-Reveals-the-Value-of-e-Commerce-in-2021.aspx

[5] สำนักงานสถิติแห่งชาติ. 2023. **ลิงค์หน่วยงาน.** [Online]. Available: http://service.nso.go.th/nso/nsopublish/link/links.html#1

[6] Blase Ur et al. 2015. “Measuring Real-World Accuracies and Biases in Modeling Password Guessability”. *In: Proceedings of the 24th USENIX Security Symposium (USENIX Security).*

[7] Christoph Breidert, Michael Hahsler and Thomas Reutterer. 2006. “A Review of Method for measuing Wllingness-to-pay.” Innovative Marketing. : 2-32

[8] D. Florêncio, C. Herley and P. C. Van Oorschot. 2014. “An administrator’s guide to internet password research.” *in 28th Large Installation System Administration Conference (Lisa14), Seattle, WA.* : 44-61.

[9] Jenjira Lomchan, Rungrat Wiangsripanawan and Siamak F. Shahandashti. 2023 “The Comparison of Password Composition Policies among US, German, and Thailand Samples.” *International Joint Conference on Computer Science and Software Engineering (JCSSE2023)*

[10] Jon A. Krosnick and Stanley Presser. 2010. “Question and Questionnaire Design. Handbook of Survey Research Second Edition.” Emerald Group Publishing Limited.

[11] Kali Linux. Common Password List. [Online] Available: https://www.kaggle.com/

datasets/wjburns/common-password-list-rockyoutxt

[12] Kevin Lee, Sten Sjöberg, and Arvind Narayanan. 2022. “Password policies of most top websites fail to follow best practices.” *in the Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). Boston, MA, USA.* : 561-580

[13] National Cyber Security Centre. 2023. **Passwords, passwords everywhere.** [Online]. Available: https://www.ncsc.gov.uk/blog-post/passwords-passwords-everywhere

[14] OpenwallProject. **Wordlistscollection**. [Online]. Available: https://www.openwall.com/wordlists/,2005.

[15] P. Mayer, J. Kirchner and M. Volkamer, 2017. “A second look at password composition policies in the wild: Comparing samples from 2010 and 2016,” *in SOUPS Thirteenth Symposium on Usable Privacy and Security*. : 13-28.

[16] Patrick Gage Kelley et al. 2012. “Guess Again (and Again and Again): Measuring Password Strength by Simulating Password-Cracking Algorithms.” *in the Proceedings of the 33rd IEEE Symposium on Security & Privacy (S&P).*

[17] Paul A. Grassi et al. 2017. “NIST Special Publication 800-63B Digital Identity Guidelines. Authentication and Lifecycle Management.”

[18] PCI Security Standards Council. 2016. “Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS).”

[19] PWC. 2023. **Thailand’s Personal Data Protection Act (PDPA): are companies in Thailand ready.** [Online]. Available: https://www.pwc.com/th/en/tax/personal-data-protection-act.html.

[20] Robert C. Hall, Mary Ann Hoppa and Yen-Hung Hu. 2023. “An Empirical Study of Password Policy Compliance.” *Journal of The Colloquium for Information Systems Security Education.* : 1-8

[21] Semrush. 2021 **Traffic Analytics.** [Online]. Available: https://developer.semrush.com/api/v3/ta/

[22] Similarweb. 2023. **Market Leaders.** [Online]. Available: https://pro.similarweb.com/#/digitalsuite/markets/webmarketanalysis/E-commerce_and_Shopping

[23] Zoominfo. 2023. **Search Retail Companies in Thailand.** [Online]. Available: https://www.zoominfo.com/companies-search/location-thailand-industry-retail

ภาคผนวก

ภาคผนวก ก.
บทความวิจัยที่ได้รับการตีพิมพ์

บทความวิจัยที่ได้รับการตีพิมพ์ในวารสารทางวิชาการระดับนานาชาติในวิทยานิพนธ์นี้มีรายละเอียดดังต่อไปนี้

[1] Jenjira Lomchan, Rungrat Wiangsripanawan and Siamak F. Shahandashti. 2023 "The Comparison of Password Composition Policies among US, German, and Thailand Samples." *International Joint Conference on Computer Science and Software Engineering (JCSSE2023)*

The 20th International Joint Conference on Computer Science and Software Engineering (JCSSE2023)

The Comparison of Password Composition Policies among US, German, and Thailand Samples

Jenjira Lomchan
Dept. of Computer Science
School of Science
King Mongkut's Institute of Technology Ladkrabang
Bangkok, Thailand
60605073@kmitl.ac.th

Rungrat Wiangsripanawan
Dept. of Computer Science.
School of Science
King Mongkut's Institute of Technology Ladkrabang
Bangkok, Thailand
rungrat.wi@kmitl.ac.th

Siamak F. Shahandashti
Dept. of Computer Science
University of York
York, United Kingdom
siamak.shahandashti@york.ac.uk

***Abstract*— The study by Mayer, Kirchner, and Volkamer published at SOUPS 2017 showed that the password composition policy (PCP) strength of both the US and German websites was not influenced by the security but by the usability features of the websites. Surprisingly, the PCP strength of the banking website category was the lowest, whereas the government website was the highest. Our aim in conducting the first study is to find whether 78 Thai frequently used websites in 2018 would yield the same surprising results. Our finding showed an opposite perspective, the highest PCP strength was from the banking websites, followed by university and government websites, respectively. Two more security features were added to our study: 2FA and HTTPS. Although some German websites employing 2FA allowed lower PCPs for better usability, Thai websites with 2FA did not loosen the password requirements. Also, employing HTTPS did not impact the PCP strength. The study with Thai websites was reinvestigated in 2021, two years after the Personal Data Protection Act (PDPA) was announced. The result showed that the median PCP strength of all Thailand samples had grown from 26.6 in 2018 to 31.0 in 2021. The banking websites still retained the highest PCP strength. A significant change appeared on the government websites, increasing from 29.9 to 40.4. In summary, the security features such as the size of services, and values of assets which play no part in both the US and German PCPs were heavily concerned by Thai websites. Government and university websites in Germany and USA gave much higher PCP strength than those in Thailand. The Thai government's PCP strength sharply increased in 2021 due to the privacy law. Nevertheless, it was still lower than the results in Germany and USA in 2016. Therefore, the criteria influencing PCP vary depending on the country.**

Keywords—Password Composition Policies (PCP), Website, Thailand

I. INTRODUCTION

Generally, all websites use username and password for authentication, and password composition policy (PCP) is often the first line of defense. Users create their passwords following the website policy. Strong policy tends to provide better security. For example, a password must be at least 8 characters with a mix of letters, numbers, and symbols.

Our research has two phases. The first phase was done in 2018 to replicate Florêncio and Herley [1] and Mayer, Kirchnerand Volkamer [2] works by exploring their mechanisms with Thailand websites. The initial objective was to compare PCPs in Thailand, Germany, and the US (data from [2]) and to find both the security and usability of website features that affected the PCP strength. By the time this study was conducted, Google had announced the move from HTTP to HTTPS. Therefore, the study also examined the strength of PCP in HTTP and HTTPS websites to find whether websites with HTTPS had better PCP strength than HTTP. In addition, as two-factor authentication (2FA) was predominantly used in websites that seem to require high security, it is added as another security feature that may influence PCP strength. As Thailand released a new privacy law called Personal Data Protection Act in 2019 [3], it is interesting to find whether the law influenced PCP strength. Hence, the same Thai websites as in the first study were reinvestigated in 2021. The aim of the second study includes whether security and usability features had changed their effects on Thai websites over three years.

Our first phase's results showed that Thailand samples generally had similar PCPs to German samples, but their policies were weaker than the US samples. Thailand gave opposite results to websites in USA and Germany. To illustrate, Thai banking websites gave the highest median PCP strength values, whereas the government websites resulted in the lowest. Unlike websites in USA and Germany that had effects from usability features: "user has choice" and "site advertises", websites in Thailand had no effect or trivial effects from these two features. A new feature like 2FA affected Thailand samples' PCP strength in 2018.

The reinvestigation in 2021, after the Ministry of Digital Economy and Society announced a new law on personal data protection in 2019, showed that 12 websites had stronger PCP strength, and 2 websites had weaker PCP strength. 61 websites did not change their PCP strength from 2018 to 2021. The government websites had improved their PCPs, but their strength was still lower than in other countries. For the security and usability features that affected the PCP strength, samples in 2021 gave similar results to samples in 2018. That is, Thailand websites did heavily concern with security features with little attention to usability features. Also, the median PCP strength of the banking websites was much higher than others, although 2FA was employed.

II. RELATED WORK

For finding Thailand website samples, a similar methodology as in Preibusch and Bonneau [4] and Seitz et al. [5] was used to find traffic rank websites from Alexa ranks to analyze top, high, medium, and medium and low website traffic. Kirchner and Volkamer [2] found that German banking website samples use 2FA for a complete payment transaction, and the PCP strength of such sites was relatively low since the security of the systems did not rely on a password only.

979-8-3503-0050-5/23/$31.00 ©2023 IEEE

TABLE I. MEDIANS OF THE FIVE SAMPLES'S PCP STRENGTH.

The median of PCP strength								
Sam-ple	Over-all	Traffic rank				Bank	Uni.	Gov.
		Top	High	Med	Low			
USA 2010	35.7	19.9	19.9	36.2	19.9	31.0	41.7	47.6
USA 2016	41.4	26.6	41.5	46.5	29.9	35.7	47.6	52.7
GER 2016	26.6	26.6	25.8	19.9	26.6	16.6	30.8	47.6
THA 2018	26.6	19.9	26.6	16.6	13.3	41.4	41.4	29.9
THA 2021	31.0	26.6	26.6	18.3	19.9	41.4	47.5	40.4

III. METHODOLOGY

Our findings in both phases replicated the study by Mayer et al. [2]. Their approach was applied to corresponding Thailand samples to compare with the original research. We added three additional attributes: method to find PCP strength, HTTPS, and 2FA. To illustrate, the "method to find PCP strength", is a way to find minimum passwords. There are (1) hints from the website and (2) the researcher did create a new account. (3) PCP documents from the website and (4) asking others to log in (such as asking the nurse to log into the Ministry of Health website). We use the Wilcoxon rank sum test [6] for finding whether the feature had affected the PCP strength. It is doubtful that the result where banking websites had the lowest PCP strength would have occurred in Thailand as well. Hence, there are 5 following questions.

RQ1: How does the PCP strength of Thailand 2018 sample compared with those in the US and German samples?

RQ2: Which website features have effects on the PCP strength of Thailand, the US, and German samples?

RQ3: Does HTTPS protocol affect the PCP strength of Thailand samples?

RQ4: Does 2FA affect the PCP strength of Thailand samples?

RQ5: Which website features that affect the PCP strength of Thailand 2021 sample change after the PDPA?

3.1 How to identify the samples of Thailand websites

Password policies from 78 Thailand websites were gathered and listed in Table I. The websites were classified into the top, high, medium, and low traffic websites, bank, university, and government websites. We used Alexa to rank 1 to 20, 100 to 110, 490 to 500, and 1000 to 1010 for the top, high, medium, and low traffic. The banks were Thailand commercial bank's highest assets in Q4 2017, provided by the Stock Exchange of Thailand [7]. We found PCPs from Internet Banking websites in the bank category. The universities were the 10 largest Thailand universities from student enrolment based on the official of the higher education commission and the top 10 of the best-rated computer science department from Thailand University Central Admission System [8]. The government websites were the 10 highest traffic websites with .go.th and .or.th at Alexa ranking. For the Thailand 2021 sample, the same websites as in the Thailand 2018 sample were reinvestigated.

3.2 Identification of PCP Strength

The PCP strength of both Thailand samples were calculated with the same method as in the original study. Where possible, we tried to create an account on the website, but if not, we would find PCP documents or hint messages on the website. For university, and government websites where we could not register an account and could not find PCP documents, we contacted officers who had accounts for their organization password policies.

3.3 Calculation of PCP strength

For finding password composition policy strength, we used the minimum strength as in [1] and [2]. The calculation is as follows:

$$\text{PCP strength} = N_{min} \times \log_2 C_{min}$$

N_{min} is the minimum length and C_{min} is the cardinality of the minimum character set required. For example, the at least 6-digit password policy strength would be $6 \times \log_2 10 \approx 19.9$ bits, whereas the at least 8-character mix of letters and digits policy strength would be $8 \times \log_2 (26+10) \approx 41.4$ bits, and the at least 8-character uppercase and lowercase letters and digits would be $8 \times \log_2 (26+26+10) \approx 47.6$ bits.

3.4 Experimental Features

Our research considered features from [1] and [2]. Security features are (1) Are Password Policies Based on Observation and Evidence? (2) What is The Size of the Service? (3) What is the Value of assets? Usability features are (1) Is Advertising Accepted? (2) Does the Site Advertise? and (3) Does the User have a Choice? We also added two additional security features: 2FA and HTTPS.

IV. RESULT

We have gathered the result of both the Thailand samples and presented them in Table I. The results of each feature including the answer to the questions are as follows:

4.1 PCP Strength

To compare PCP strength of each country, we use their median values as in [1] and [2]. The overall PCP strength of Thailand 2018 sample was 26.6 bits which was equal to the German 2016 sample. Table I shows the value of PCP strength of each category in all samples. As previous work, the median values are used to represent the PCP strength of each sample.

4.2 Size of the Service

Table II shows the number of active users and PCP strength of selected websites from Thailand 2018 sample. The first five rows were the most popular sites as of 2018 [9], based on the number of users. The last five rows were the university websites chosen from the top five with the highest number of students enrolled in 2018 [10]. Google, which ranked No. 1 and had the highest number of users, gave PCP strength at 26.6. Prince of Songkla gave higher PCP values (47.5) than Ramkhamhaeng (26.6), although their number of users was 5 times lower. Hence, the size of the service obviously has no effect on the PCP strengths.

TABLE II. NO. OF ACTIVE USERS AND PCP STRENGTH OF THAILAND 2018 SAMPLE (TOP TRAFFIC WEBSITES AND LARGE UNIVERSITY WEBSITES).

Size of service			
Site	**Users**	**Rank**	**Min. Strength**
Gmail	1.5 B	1	26.6
Facebook	2.2 B	4	19.9
Line	0.2 B	8	31
Lazada	8 M	9	31
Pantip	5 M	5	19.9
Ramkhamhaeng	222,023	252	26.6
Kasetsart	66,726	67	41.4
Sukhothai Thammathirat	61,935	259	59.5
Mahasarakham	45,273	268	13.3
Prince Of Songkla	40,443	88	47.6

4.3 Value of Assets

Thailand 2018 and 2021 samples show the opposite results for bank and government websites from those in the US and German samples. Table I shows the median PCP strength of each category for all samples. Thailand banking websites had the highest (41.4 bits), but their government websites had the lowest PCP strength of all five samples (29.9 bits in 2018 and 40.4 in 2021).

4.4 Advertising Accepted

Some websites accepted third-party advertisements to earn some money, but others do not. Table III shows whether a website accepts advertisements from a third party or not. Most top-traffic websites supported ads, whereas bank, university, and government websites did not. A Wilcoxon rank sum test indicated that websites displaying third-party advertisements had significantly weaker PCP strength than those that did not display advertisements in the Thailand 2018 sample ($W = 1000$, $p < 0.001$) and the Thailand 2021 sample ($W = 1000$, $p < 0.001$ in 2018 sample and $W = 1058.5$, $p = <0.001$ in 2021 sample).

4.5 Site Advertises

Some websites place advertisements on other websites to increase their traffic. We used Google Ads for tabulating whether a website placed advertisements on other websites or not. Table I shows this result. All top-traffic websites placed advertisements where bank, university, and government websites did not. A Wilcoxon rank sum resulted in a rejection of the hypothesis that there was a difference in PCPs between websites placed advertises on other websites and those that did not in the Thailand samples ($W = 447$, $p = 0.4777$ in the 2018 sample and $W = 339.5$, $p = 0.8261$ in 2021 sample).

4.6 User Has Choice

Many sites such as Facebook and Google, their users have a choice to choose the websites' services. All five samples from USA 2010, USA 2016 ($W = 976.5$, $p < 0.001$), German 2016 ($W = 780.0$, $p = 0.004$), Thailand 2018 ($W = 1174$, $p < 0.0001$), and Thailand 2021 ($W = 1123$, $p < 0.0001$) show that all samples that implemented this feature have lower PCP strength. None of the government websites in all samples allowed this feature. None of the banking websites except PayPal in Germany and USA allowed this feature either. To emphasize for Thailand 2018 and 2021 samples, this feature was not allowed on government and bank websites at all in both samples.

4.7 HTTPS Protocol

Nowadays, many websites use HTTPS to increase the security of data transmission. Table IV shows PCPs and websites whether they used HTTPS or not. For Thailand 2018 sample, all bank and top traffic websites used HTTPS. Most websites for each category used HTTPS except the government. For Thailand 2021 sample, all government websites used HTTPS. A Wilcoxon rank sum test supported this finding, resulting in a rejection of the hypothesis that there was a difference in PCPs between websites using and not using HTTPS protocol l in the Thailand samples ($W = 569$, $p = 0.7315$ in the 2018 sample and $W = 8$, $p = 0.0327$ in 2021 sample).

4.8 Two Factor Authentication (2FA)

Since the 2018 sample, all Thailand bank websites required 2FA or two-step verification to increase their website security. Unlike the German sample, the median PCPs of these websites were still very high and higher than non 2FA websites. Since the Bank of Thailand introduced a new regulation to facilitate the Know-Your-Customer (KYC) process for account opening. All bank websites using KYC for account opening must use 2FA for payment transactions via Internet Banking websites. In 2021, any website with an online payment method must have a KYC process to make the payment transaction. For example, the Lazada website requires two-step authentications for opening an e-wallet account and requires 2FA for purchasing above 1,000 baht. Email services and social media websites also provide 2FA in addition to passwords such as OTP, authentication apps, and security keys.

Consequently, this finding is supported by a Wilcoxon rank sum resulting in accepting the hypothesis that there is a difference in PCPs between 2FA-deployed websites and 2FA-nondeployed websites ($W = 228$, $p = 0.008$ in the 2018 sample and $W = 251$, $p = 0.0163$ in 2021 sample).

4.9 Password Policies based on Observation and Evidence

We used the same methodology as the Mayer, Kirchner and Volkamer [2] study to find password breaches or leaked data. We found that only one website increased the PCP strength after the found breach (booking.com) [11]–[19]. The other 10 websites remain unchanged as some websites already set higher PCP strength and enforce 2FA. There are 13 websites that did not find a password-related breach or leak but increased the PCP strength.

V. DISCUSSION

We investigated the effects of website features to compare the PCPs in different countries and over time. We discuss the finding answer to our research question in the following.

TABLE III. THE MEDIAN PCPS ACCORDING TO USABILITY FEATURES.

Sample	**User choice**		**Advertises**		**Accepts ads**	
	Yes	**No**	**Yes**	**No**	**Yes**	**No**
USA 2010	19.9	41.6	31.0	35.7	19.9	41.1
USA 2016	26.6	47.6	47.6	41.4	19.9	47.6
GER 2016	26.2	31.0	22.9	26.6	26.6	26.6
THA 2018	19.9	41.4	26.6	26.6	19.9	32.1
THA 2021	21.6	41.4	28.8	33.2	31.0	41.4

5.1 How does the PCP strength of Thailand 2018 sample compared with those in the US and German samples?

In this question, Thailand 2018 sample is compared with the US and German samples using the median PCP strength value of each website category. As can be seen in Table I, the overall PCP strength of the Thailand 2018 sample (26.6) is equal to the German 2016 sample and lower than the US samples (35.7 and 41.4). For top-traffic rank websites, the PCP strength of Thailand 2018 sample (19.9) is equal to the USA 2010 sample and lower than other samples (26.6). For high-traffic rank websites, the PCP strength of Thailand 2018 sample (26.6) is lower than the USA 2016 sample (41.5) but higher than other samples (19.9 and 25.8). For medium and low-traffic rank websites, the PCP strength of Thailand 2018 sample gives the lowest values which are 16.6 and 13.3, respectively. For the university websites, the PCP strength of Thailand 2018 sample (41.4) is higher than the German 2016 sample (30.8) but is lower value than both USA samples (31.0 and 35.7). Banking website category in the Thailand 2018 sample has the highest PCP strength (41.4). This value is much higher than other samples especially the German 2016 sample (16.6). In contrary, the Thailand 2018 government category has the lowest PCP strength (29.9) comparing with the USA 2010 and the German 2016 (47.6) and the USA 2016 (52.7).

5.2 Which website features have effects on the PCP strength of Thailand, the US, and German samples?

As shown in [2], security features did not affect the PCP strength of samples in US and Germany, but usability features did. However, the security features greatly affected the PCP strength of Thailand samples. Features like *Site of Service* and *value of resource protected* heavily influenced banking websites in Thailand. Unlike Germany and the US, their banking websites had the lowest PCP strength, and the PCP strength of Thai banking websites were the highest. Even though 2FA was deployed, the Thai banking websites' PCP was still very high. Conversely, the Thai government websites had the lowest values whereas the US and German government websites' PCP strength were the highest. The *Advertising accepted* affected the PCP strength in both Thailand and USA but not in German. *Site Advertises* did not affect the PCPs in Thailand. *User has choice* feature affected the PCP strength in all five samples for websites that implemented this feature.

5.3 Does HTTPS protocol affect the PCP strength of Thailand samples?

HTTPS protocol is not affecting the PCP strength in the Thailand sample. The result of our study shows a combination of PCPs between that website using HTTPS protocol and not using HTTPS protocol. Some websites use this feature but still have low PCP strength and some websites not using that have PCPs is high. However, our results show almost websites in top-traffic, high-traffic, medium-traffic, university, and bank websites use HTTPS. For government websites, the 2018 sample found 5 in 8 websites not using that, and in the 2021 sample all government websites used HTTPS.

5.4 Does 2FA affect the PCP strength of Thailand samples?

2FA had affected the PCP strength in the Thailand samples. Websites that require this feature would have very high PCP strength. These websites provided mostly provided online payment transactions such as banks and e-commerce websites. The median PCP strength of the 2FA websites was higher than non-2FA websites. It is the opposite result from Mayer, Kirchner and Volkamer [2]. Their study concluded for German samples with 2FA that PCP strength could become smaller because 2FA was implemented. For Thailand samples, apart from bank websites, there were 2 websites (lazada.co.th and rd.go.th) in 2021 that changed to use 2FA, and PCP strength is still high.

5.5 Which website features which affecting the PCP strength of Thailand 2021 sample change after the PDPA?

The median PCP strength of the Thailand samples has grown significantly from 26.6 bits in 2018 to 31.0 bits in 2021. The increase in median PCP strength is caused by 12 websites changing to have stronger PCPs. However, there were 2 websites having weaker PCPs. The remaining 61 websites did not change their PCPs from 2018 to 2021. For the PCP strength of the government websites, it has increased from 29.9 bits in 2018 to 40.4 bits in 2021. In 2019, the Ministry of Digital Economy and Society announced a new law on personal data protection (PDPA). Consequently, most organizations were conscious of collecting and disclosing personal information, so they improved their website security. Increasing PCP strength is one of the mechanisms used. As can be seen in Table IV, the websites such as the Revenue Department (government), Kiatnakin Bank, and Chiangmai University had significantly improved their website PCP strength from 26.6 to 47.6, 19.9 to 41.4, and 19.9 to 47.4 bits, respectively.

According to information in subsections 4.2 to 4.9, features that affect or do not affect the PCP strength of Thailand 2021 sample remain the same features as in 2018 sample. Therefore, the rising PCP strength of the Thailand 2021 sample is likely to be influenced by the PDPA law.

VI. Conclusion

We presented a replication of the study by Mayer, Kirchner and Volkamer [2] to answer two research questions: (1) a comparison of password composition policies across country borders, (2) a comparison of website features that affect PCP strength across country borders. And answer our research questions, whether (3) HTTPS protocol and (4) 2FA affect PCP strength in the Thailand sample or not.

For the first contribution, the overall PCPs of the Thailand and German samples are equal and lower than the USA samples. Thailand bank websites show the highest PCP strength, but government websites give the lowest PCP strength of all samples. For the second contribution, User has choice has affected the PCP strength of all samples, but the Site advertises does not. Advertising accepted has affected the PCP strength in the Thailand and USA samples but does not affect the German sample. HTTPS protocol does not affect the PCP strength in the Thailand sample but 2FA has. Lastly, the PCP strength of the Thailand sample has grown significantly from 2018 to 2021 possibly due to the PDPA law.

References

[1] D. Florêncio, C. Herley and P. C. Van Oorschot, "An administrator's guide to internet password research," in *28th Large Installation System Administration Conference (Lisa14)*, Seattle, WA, 2014, pp. 44-61.

[2] P. Mayer, J. Kirchner and M. Volkamer, "A second look at password composition policies in the wild: Comparing samples from 2010 and 2016," in *SOUPS Thirteenth Symposium on Usable Privacy and Security*, July 12–14, 2017, Santa Clara, CA, USA, Santa Clara, CA, USA, 2017, pp. 13-28.

[3] PWC. (2023, Mar. 1). *Thailand's Personal Data Protection Act (PDPA): are companies in Thailand ready* [Online]. Available: https://www.pwc.com/th/en/tax/personal-data-protection-act.html.

[4] P. G. Kelley, S. Komanduri, M. L. Mazurek, R. Shay, T. Vidas, L. Bauer, N. Christin, L. F. Cranor and J. Lopez, "Guess again (and again and again): neasuring password strength by simulating password-Cracking algorithms," in *2012 IEEE Symposium on Security and Privacy*, San Francisco, CA, USA, May 2012, pp. 523-537.

[5] T. Seitz, M. Hartmann, J. Pfab, and S. Souque, "Do Differences in Password Policies Prevent Password Reuse?" *Proceedings of the 2017 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, New York, NY, USA, 2017, pp. 2056-2063.

[6] The R Stats Package. (2019, Jan. 6). *R: Wilcoxon Rank Sum and signed rank tests* [Online]. Available: https://stat.ethz.ch/R-manual/R-devel/library/stats/html/wilcox.test.html.

[7] SET. (2019, Jan. 19). *Stock Exchange of Thailand* [Online]. Available: https://www.set.or.th.

[8] TCAS66. (2018, Nov. 30). *Thai university Central Admission System* [Online]. Available: http://www.mytcas.com.

[9] Statista. (2019, Feb. 5). *Most popular social networks worldwide as of 2018* [Online]. Available: https://www.statista/statistics/272014/global-social-networks-ranked-by-number-of-users.

[10] Ministry of Higher Education, Science, Research, and Innovation. (2018, Nov. 30). *Official of the higher education commission* [Online]. Available: http://www.info.mua.go.th.

[11] A. Holmes. (2023). *533 million Facebook users' phone numbers and personal data leak* [Online]. Available: https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online.

[12] Reuters. (2023, Mar. 1). *Krung Thai, Kasikorn report data leak.* [Online]. Available: https://www.reuters.com/article/thailand-banks-idUSL4N1UR4RV.

[13] Thai Enquirer. (2023, Mar. 1). *Lazada blames third party for data leak* [Online]. Available: https://www.thaienquirer.com/20953/lazada-suffers-data-hack-of-13-million-accounts.

[14] Lifelock. (2023, Mar. 1). *Microsoft exposed 250 million customer records* [Online]. Available: https://lifelock.norton.com/learn/databreaches/microsoft-exposed-250-million-customer.

[15] Cisomag. (2023, Mar. 1). *Instagram data breach! 49 million users' sensitive data exposed* [Online]. Available: https://cisomag.com/instagram-data-breach-49-million-users-sensitive-data-exposed.

[16] NCSC. (2023, Mar. 1). *Data breach of 500m Yahoo accounts* [Online]. Available: https://www.ncsc.gov.uk/news/data-breach-500m-yahoo-accounts.

[17] M. X. Heiligenstein. (2023). *Twitter Data Breaches: Full Timeline* [Online]. Available: https://firewalltimes.com/twitter-data-breach-timeline.

[18] CPO Magazine. (2023, Mar. 1). *Data Leak at Hotel Booking Companies Affected Millions of Guests* [Online]. Available: https://www.cpomagazine.com/cyber-security/data-leak-at-hotel-booking-affected-millions-of-guests.

[19] Bangkok Post. (2023, Mar. 1). *3-week lapse for AIS data breach* [Online]. Available: https://www.bangkokpost.com/business/3-week-lapse-for-ais-data-breach.

TABLE IV. THE THAILAND WEBSITE SAMPLE THA 2018 AND THA 2021 COMPRISING 78 WEBSITES. TRAFFIC RANKS ACCORDING TO ALEXA.

Website	Traffic Rank	MTFI[6]	Min. Length		Size Charset		Min. Strength		Accept Ads?		Places Ads?		User Choice		HTTPS		2FA[7]	
			2018	2021	2018	2021	2018	2021	2018	2021	2018	2021	2018	2021	2018	2021	2018	2021
Top Traffic Sites																		
google.co.th[2]	1	A	8	8	10	10	26.6	26.6	y	y	n	n	y	y	y	y	O	O
facebook.com[3]	4	A	6	6	10	10	19.9	19.9	y	y	y	y	y	y	y	y	O	O
pantip.com	5	A	6	6	10	10	19.9	19.9	y	y	n	n	y	y	y	y	O	O
line.me	8	A	6	6	36	36	31.0	31.0	y	y	y	y	y	y	y	y	M	M
lazada.co.th	9	A	6	6	36	36	31.0	31.0	n	n	y	y	y	y	y	y	-	M
live.com	10	A	8	8	36	36	41.4	41.4	y	y	n	n	y	y	y	y	-	O
wikipedia.org	11	A	1	8	10	10	3.3	26.6	n	n	n	n	y	y	y	y	-	-
sanook.com	12	A	6	6	10	10	19.9	19.9	y	y	n	n	y	y	y	y	-	-
instagram.com	13	A	6	6	10	10	19.9	19.9	y	y	n	n	y	y	y	y	O	O
kapook.com	14	A	6	6	10	10	19.9	19.9	y	y	n	n	y	y	y	y	-	-
yahoo.com	15	A	9	9	10	10	29.9	29.9	y	y	n	n	y	y	y	y	-	O
twitter.com	16	A	6	8	10	10	19.9	26.6	y	y	n	n	y	y	y	y	-	O
shopee.co.th	18	A	8	8	52	52	45.6	45.6	n	n	y	y	y	y	y	y	M	M
wordpress.com	19	A	9	9	26	26	42.3	42.3	y	y	y	y	y	y	y	y	-	-
dek-d.com	20	A	6	4	10	10	19.9	13.3	y	y	n	n	y	y	y	y	-	-
High Traffic Site																		
agoda.com	100	A	8	8	10	10	26.6	26.6	y	y	y	y	y	y	y	y	-	-
ais.co.th	103	A	8	8	62	62	47.6	47.6	n	n	n	n	y	y	y	y	M	M
shutterstock.com	104	A	8	8	10	10	26.6	26.6	n	n	y	y	y	y	y	y	-	-
booking.com	105	A	8	10	10	62	26.6	59.5	n	n	y	y	y	y	y	y	-	-
pinterest.com	106	A	6	7	10	10	19.9	23.3	n	n	n	n	y	y	y	y	-	-
notebookspec.com[8]	107	A	4		10		13.3		y		y		y		y		-	
mahidol.ac.th	108	H	8	8	36	36	41.4	41.4	n	n	n	n	y	y	n	y	-	-
tunwalai.com	109	A	4	4	10	10	13.3	13.3	y	y	y	y	y	y	n	n	-	-
nanamovies.com	110	A	5	5	10	10	16.6	16.6	n	n	n	n	y	y	y	y	-	-
Medium Traffic Sites																		
jobtopgun.com	490	A	6	6	10	10	19.9	19.9	y	y	y	y	y	y	y	y	-	-
sritown.com	492	A	4	4	10	10	13.3	13.3	y	y	n	n	y	y	n	y	-	-
efinancethai.com	493	A	4	4	10	10	13.3	13.3	y	y	n	n	y	y	n	y	-	-
asus.com	495	A	8	8	10	10	26.6	26.6	n	n	n	n	y	y	y	y	-	-
fictionlog.co	496	A	6	6	10	10	19.9	19.9	n	n	n	n	y	y	y	y	-	-

Website	Traffic Rank	MTFI[6]	Min. Length		Size Charset		Min. Strength		Accept Ads?		Places Ads?		User Choice		HTTPS		2FA[7]	
			2018	2021	2018	2021	2018	2021	2018	2021	2018	2021	2018	2021	2018	2021	2018	2021
theasianparent.com	497	A	6	6	10	10	19.9	19.9	n	y	n	n	y	y	y	y	-	-
hdzog.com	498	A	5	5	10	10	16.6	16.6	y	y	n	n	y	y	y	y	-	-
ookbeecomics.com	499	A	4		10		13.3		n		y		y		n		-	
online-station.net	500	A	5	5	10	10	16.6	16.6	y	y	n	y	y	y	y	y	-	-
Low Traffic Sites																		
dotproperty.co.th	1001	A	6	6	10	10	19.9	19.9	y	y	n	n	y	y	y	y	-	-
11street.co.th	1002	A	6	6	36	36	31.0	31.0	n	n	n	n	y	y	y	y	-	-
thailandsusu.com	1004	A	4	4	10	10	13.3	13.3	y	y	n	n	y	y	n	n	-	-
forexfactory.com	1005	A	1	1	10	10	3.3	3.3	y	y	n	n	y	y	y	y	-	-
pastebin.com	1008	A	4	12	10	10	13.3	39.9	n	y	n	n	y	y	y	y	-	-
thaithesims4.com	1009	A	3	3	10	10	10.0	10.0	y	y	n	n	y	y	n	y	-	-
tradingview.com	1010	A	7	7	36	36	36.2	36.2	n	n	n	n	y	y	y	y	-	-
Bank																		
Bangkok Bank	1	A	8	8	36	36	41.4	41.4	n	n	n	n	n	n	y	y	M	M
Siam Commercial Bank	2	C	8	8	36	36	41.4	41.4	n	n	n	n	n	n	y	y	M	M
Kasikorn Bank	3	A	8	8	36	36	41.4	41.4	n	n	n	n	n	n	y	y	M	M
Tisco Bank	4	P	8	8	88	88	51.7	51.7	n	n	n	n	n	n	y	y	M	M
Thanachart Bank[9]	5	P	6		10		19.9		n		n		n		y		M	
Kiatnakin Bank	6	P	6	8	10	36	19.9	41.4	n	n	n	n	n	n	y	y	M	M
Bank of Ayudhya	7	A	8	8	10	36	26.6	41.4	n	n	n	n	n	n	y	y	M	M
Krungthai Bank	8	P	8	8	62	36	47.6	41.4	n	n	n	n	n	n	y	y	M	M
Land and House Bank	9	P	8	8	36	36	41.4	41.4	n	n	n	n	n	n	y	y	M	M
TMB Bank[9]	10	H	8	8	36	36	41.4	41.4	n	n	n	n	n	n	y	y	M	M
Large Universities																		
Ramkhamhaeng	222023	C	8	8	10	10	26.6	26.6	n	n	n	n	n	n	y	y	-	-
Kasetsart	66726	C	8	8	36	62	41.4	47.6	n	n	n	n	n	n	y	y	-	-
Sukhothai Thammathirat	61935	C	10	10	62	62	59.5	59.5	n	n	n	n	n	n	y	y	-	-
Mahasarakham	45273	C	4	4	10	10	13.3	13.3	n	n	n	n	n	n	y	y	-	-
Prince Of Songkla	40443	H	8	8	62	64	47.6	48.0	n	n	n	n	n	n	y	y	-	-
Khonkaen	38722	C	10	10	62	62	59.5	59.5	n	n	n	n	n	n	y	y	-	-
Chulalongkorn	37036	C	6	6	10	10	19.9	19.9	n	n	n	n	n	n	y	y	-	-
Thammasat	36166	C	6	6	10	10	19.9	19.9	n	n	n	n	n	n	y	y	-	-
Chiangmai	36117	C	6	8	10	61	19.9	47.4	n	n	n	n	n	n	y	y	-	-
Burapha	33940	H	8	8	62	67	47.6	48.5	n	n	n	n	n	n	y	y	-	-
Universities with top CS departments																		
Chulalongkorn	282	C	6	6	10	10	19.9	19.9	n	n	n	n	n	n	y	y	-	-
Kasetsart	1582	C	8	8	36	62	41.4	47.6	n	n	n	n	n	n	y	y	-	-
Thammasat	532	C	6	6	10	10	19.9	19.9	n	n	n	n	n	n	y	y	-	-
Chiangmai	554	C	6	8	10	61	19.9	47.4	n	n	n	n	n	n	y	y	-	-
KMITL	739	A	8	10	36	62	41.4	59.5	n	n	n	n	n	n	n	y	-	-
KMUTT	307	C	8	8	62	77	47.6	50.1	n	n	n	n	n	n	n	y	-	-
Khonkaen	622	C	10	10	62	62	59.5	59.5	n	n	n	n	n	n	y	y	-	-
Srinakharinwirot	184	C	8	8	36	36	41.4	41.4	n	n	n	n	n	n	y	y	-	-
Silpakorn	266	C	8	8	62	62	47.6	47.6	n	n	n	n	n	n	y	y	-	-
Burapha	554	C	8	8	62	67	47.6	48.5	n	n	n	n	n	n	n	y	-	-
Government Sites																		
moph.go.th	86	C	8	8	62	62	47.6	47.6	n	n	n	n	n	n	y	y	-	-
obec.go.th	126	H	10	10	10	10	33.2	33.2	n	n	n	n	n	n	n	y	-	-
gprocurement.go.th	153	H	7	7	10	10	23.3	23.3	n	n	n	n	n	n	n	y	-	-
rd.go.th	298	P	8	8	10	62	26.6	47.6	n	n	n	n	n	n	n	y	-	M
ocsc.go.th	310	H	6	6	10	10	19.9	19.9	n	n	n	n	n	n	y	y	-	-
dbd.go.th	383	H	8	8	62	62	47.6	47.6	n	n	n	n	n	n	n	y	-	-
glo.or.th	408	P	8	8	36	62	41.4	47.6	n	n	n	n	n	n	n	y	-	-
sso.go.th	445	H	6	6	10	10	19.9	19.9	n	n	n	n	n	n	y	y	-	-

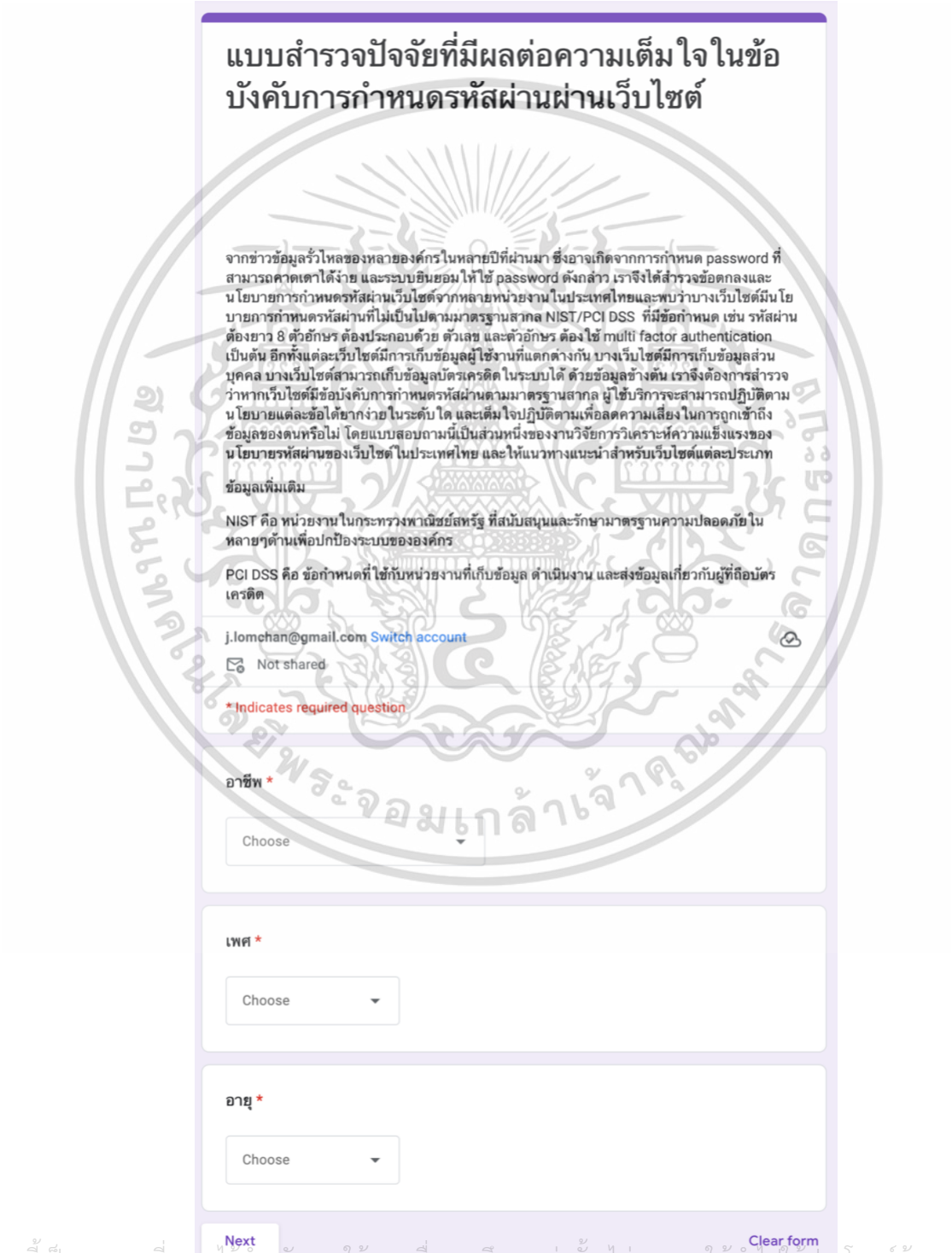
. Traffic info from Alexa.com. We investigated password policies for sites 1-20, 100-110, 490-500, 1000-1010, and for the top 10 government sites. We di not find policies for sites #6 (Movie2free.com), #17 (Thairath.co.th), #101 (Thailandpost.co.th), #175 (Tmd.go.th), #419 (Nhso.go.th), #491 (Dontaree.com) #1003 (Aelitaxtranslate.com), #1006 (Thaijobsgov.com), #1007 (beinsport4k.com).
. Google Account is also used on the site Google.co.th (#1), Youtube.com (#2), Google.com (#3), and Blogspot.com (#7).
. Facebook Account is also used on the site Bugaboo.tv (#102) and Vonvon.me (#494).
. Top 10 Thailand universities by 2018 enrollment.
. Top CS Depts as top 10 admission.
. The mean for MTFI (Methods to find it) H is Hints found in the websites, A is Created accounts, P is found in the PCP documents, C is Crowdsourced
. The mean for 2FA (Two-factor authentication) O is Optional, M is Mandatory, and "-" is websites that do not identify two-factor authentication.
. notebookspec.com and ookbeecomics.com websites have been discontinued.
. Thanachart Bank and TMB Bank merge company and use the same website

ภาคผนวก ข.

แบบสอบถามที่ใช้ในงานวิจัย

แบบสอบถามที่ใช้ในงานวิจัยนี้ทั้งหมด 2 แบบสอบถาม ดังนี้

1. แบบสำรวจปัจจัยที่มีผลต่อความเต็มใจในข้อบังคับการกำหนดรหัสผ่านผ่านเว็บไซต์



แบบสำรวจปัจจัยที่มีผลต่อความเต็มใจในข้อบังคับการกำหนดรหัสผ่านผ่านเว็บไซต์

จากข่าวข้อมูลรั่วไหลขององค์กรในหลายปีที่ผ่านมา ซึ่งอาจเกิดจากการกำหนด password ที่สามารถคาดเดาได้ง่าย และระบบยินยอมให้ใช้ password ดังกล่าว เราจึงได้สำรวจข้อตกลงและนโยบายการกำหนดรหัสผ่านเว็บไซต์จากหลายหน่วยงานในประเทศไทยและพบว่าบางเว็บไซต์มีนโยบายการกำหนดรหัสผ่านที่ไม่เป็นไปตามมาตรฐานสากล NIST/PCI DSS ที่มีข้อกำหนด เช่น รหัสผ่านต้องยาว 8 ตัวอักษร ต้องประกอบด้วย ตัวเลข และตัวอักษร ต้องใช้ multi factor authentication เป็นต้น อีกทั้งแต่ละเว็บไซต์มีการเก็บข้อมูลผู้ใช้งานที่แตกต่างกัน บางเว็บไซต์มีการเก็บข้อมูลส่วนบุคคล บางเว็บไซต์สามารถเก็บข้อมูลบัตรเครดิตในระบบได้ ด้วยข้อมูลข้างต้น เราจึงต้องการสำรวจว่าหากเว็บไซต์มีข้อบังคับการกำหนดรหัสผ่านตามมาตรฐานสากล ผู้ใช้บริการจะสามารถปฏิบัติตามนโยบายแต่ละข้อได้ยากง่ายในระดับใด และเต็มใจปฏิบัติตามเพื่อลดความเสี่ยงในการถูกเข้าถึงข้อมูลของตนหรือไม่ โดยแบบสอบถามนี้เป็นส่วนหนึ่งของงานวิจัยการวิเคราะห์ความแข็งแรงของนโยบายรหัสผ่านของเว็บไซต์ในประเทศไทย และให้แนวทางแนะนำสำหรับเว็บไซต์แต่ละประเภท

ข้อมูลเพิ่มเติม

NIST คือ หน่วยงานในกระทรวงพาณิชย์สหรัฐ ที่สนับสนุนและรักษามาตรฐานความปลอดภัยในหลายๆด้านเพื่อปกป้องระบบขององค์กร

PCI DSS คือ ข้อกำหนดที่ใช้กับหน่วยงานที่เก็บข้อมูล ดำเนินงาน และส่งข้อมูลเกี่ยวกับผู้ที่ถือบัตรเครดิต

j.lomchan@gmail.com Switch account

Not shared

* Indicates required question

อาชีพ *

Choose

เพศ *

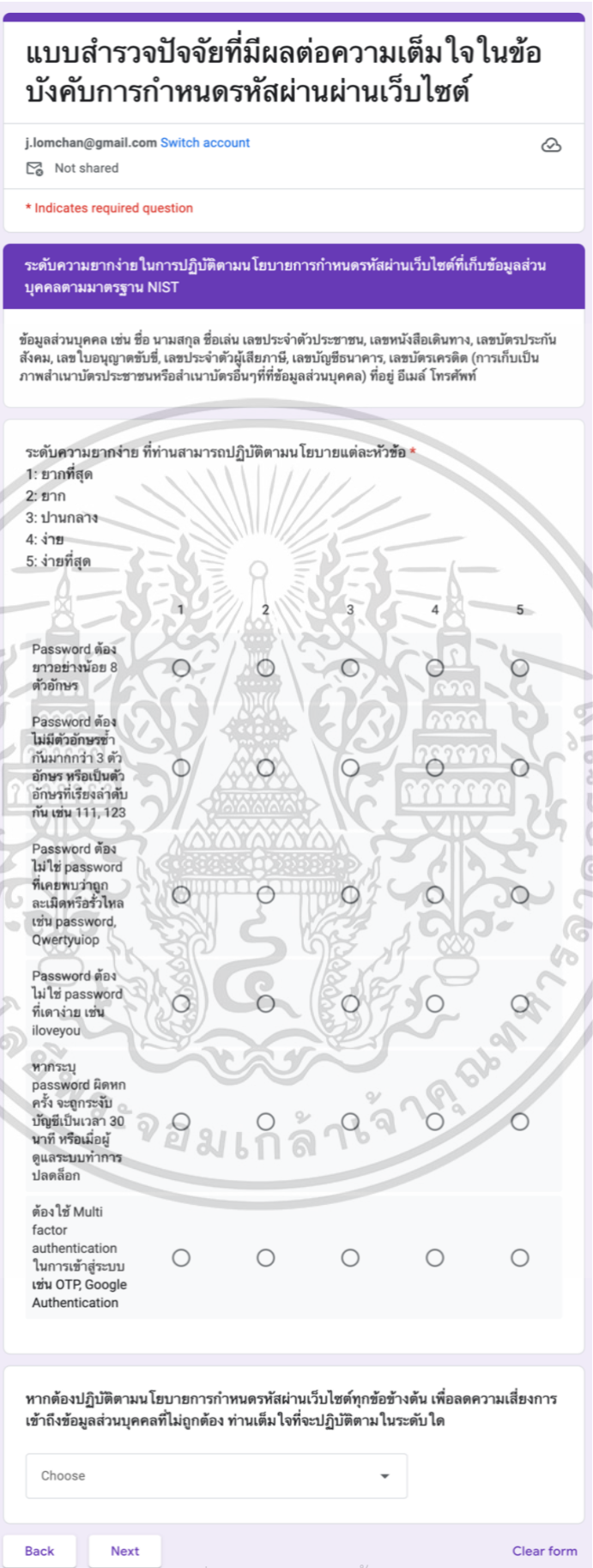
Choose

อายุ *

Choose

Next

Clear form



แบบสำรวจปัจจัยที่มีผลต่อความเต็มใจในข้อบังคับการกำหนดรหัสผ่านผ่านเว็บไซต์

j.lomchan@gmail.com Switch account

Not shared

* Indicates required question

ระดับความยากง่ายในการปฏิบัติตามนโยบายการกำหนดรหัสผ่านเว็บไซต์ที่เก็บข้อมูลส่วนบุคคลตามมาตรฐาน NIST

ข้อมูลส่วนบุคคล เช่น ชื่อ นามสกุล ชื่อเล่น เลขประจำตัวประชาชน, เลขหนังสือเดินทาง, เลขบัตรประกันสังคม, เลขใบอนุญาตขับขี่, เลขประจำตัวผู้เสียภาษี, เลขบัญชีธนาคาร, เลขบัตรเครดิต (การเก็บเป็นภาพสำเนาบัตรประชาชนหรือสำเนาบัตรอื่นๆที่ที่ข้อมูลส่วนบุคคล) ที่อยู่ อีเมล์ โทรศัพท์

ระดับความยากง่าย ที่ท่านสามารถปฏิบัติตามนโยบายแต่ละหัวข้อ *

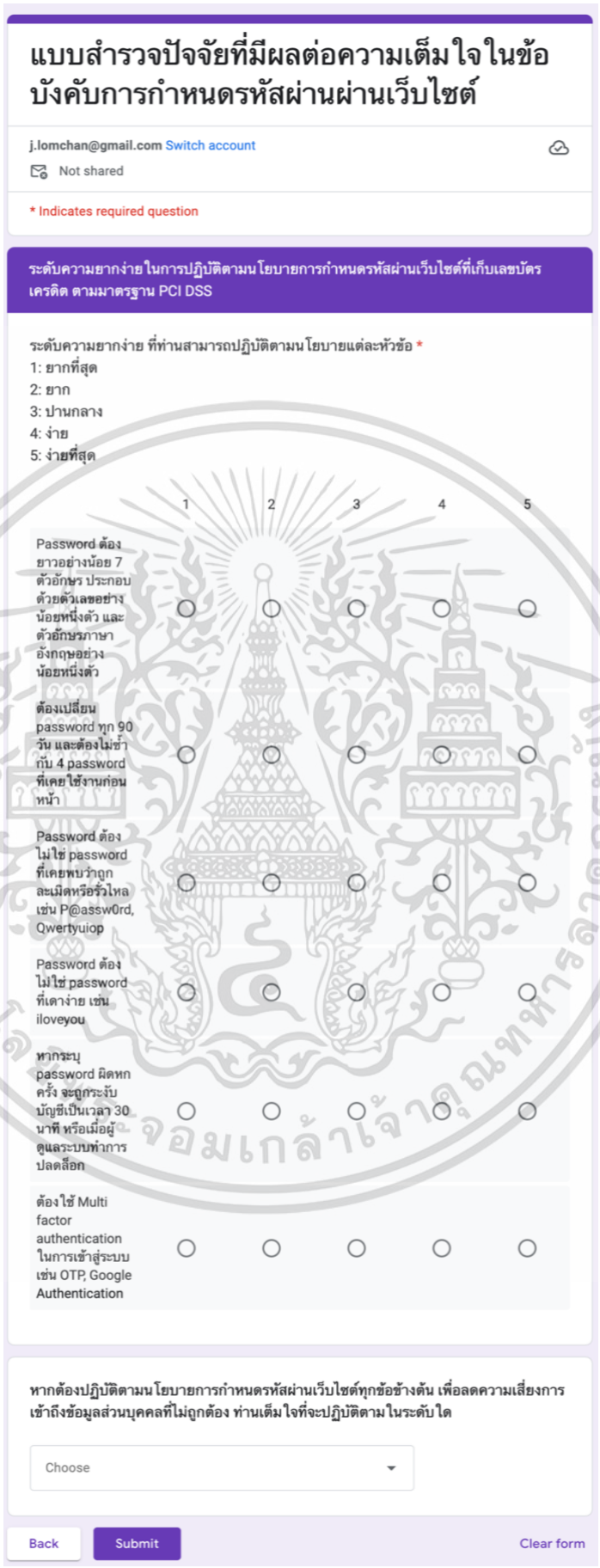
1: ยากที่สุด
2: ยาก
3: ปานกลาง
4: ง่าย
5: ง่ายที่สุด

	1	2	3	4	5
Password ต้องยาวอย่างน้อย 8 ตัวอักษร	○	○	○	○	○
Password ต้องไม่มีตัวอักษรซ้ำกันมากกว่า 3 ตัวอักษร หรือเป็นตัวอักษรที่เรียงลำดับกัน เช่น 111, 123	○	○	○	○	○
Password ต้องไม่ใช่ password ที่เคยพบว่าถูกละเมิดหรือรั่วไหล เช่น password, Qwertyuiop	○	○	○	○	○
Password ต้องไม่ใช่ password ที่เดาง่าย เช่น iloveyou	○	○	○	○	○
หากระบุ password ผิดหกครั้ง จะถูกระงับบัญชีเป็นเวลา 30 นาที หรือเมื่อผู้ดูแลระบบทำการปลดล็อก	○	○	○	○	○
ต้องใช้ Multi factor authentication ในการเข้าสู่ระบบ เช่น OTP, Google Authentication	○	○	○	○	○

หากต้องปฏิบัติตามนโยบายการกำหนดรหัสผ่านเว็บไซต์ทุกข้อข้างต้น เพื่อลดความเสี่ยงการเข้าถึงข้อมูลส่วนบุคคลที่ไม่ถูกต้อง ท่านเต็มใจที่จะปฏิบัติตามในระดับใด

Choose

Back Next Clear form



แบบสำรวจปัจจัยที่มีผลต่อความเต็มใจในข้อบังคับการกำหนดรหัสผ่านผ่านเว็บไซต์

j.lomchan@gmail.com Switch account

Not shared

* Indicates required question

ระดับความยากง่ายในการปฏิบัติตามนโยบายการกำหนดรหัสผ่านเว็บไซต์ที่เก็บเลขบัตรเครดิต ตามมาตรฐาน PCI DSS

ระดับความยากง่าย ที่ท่านสามารถปฏิบัติตามนโยบายแต่ละหัวข้อ *
1: ยากที่สุด
2: ยาก
3: ปานกลาง
4: ง่าย
5: ง่ายที่สุด

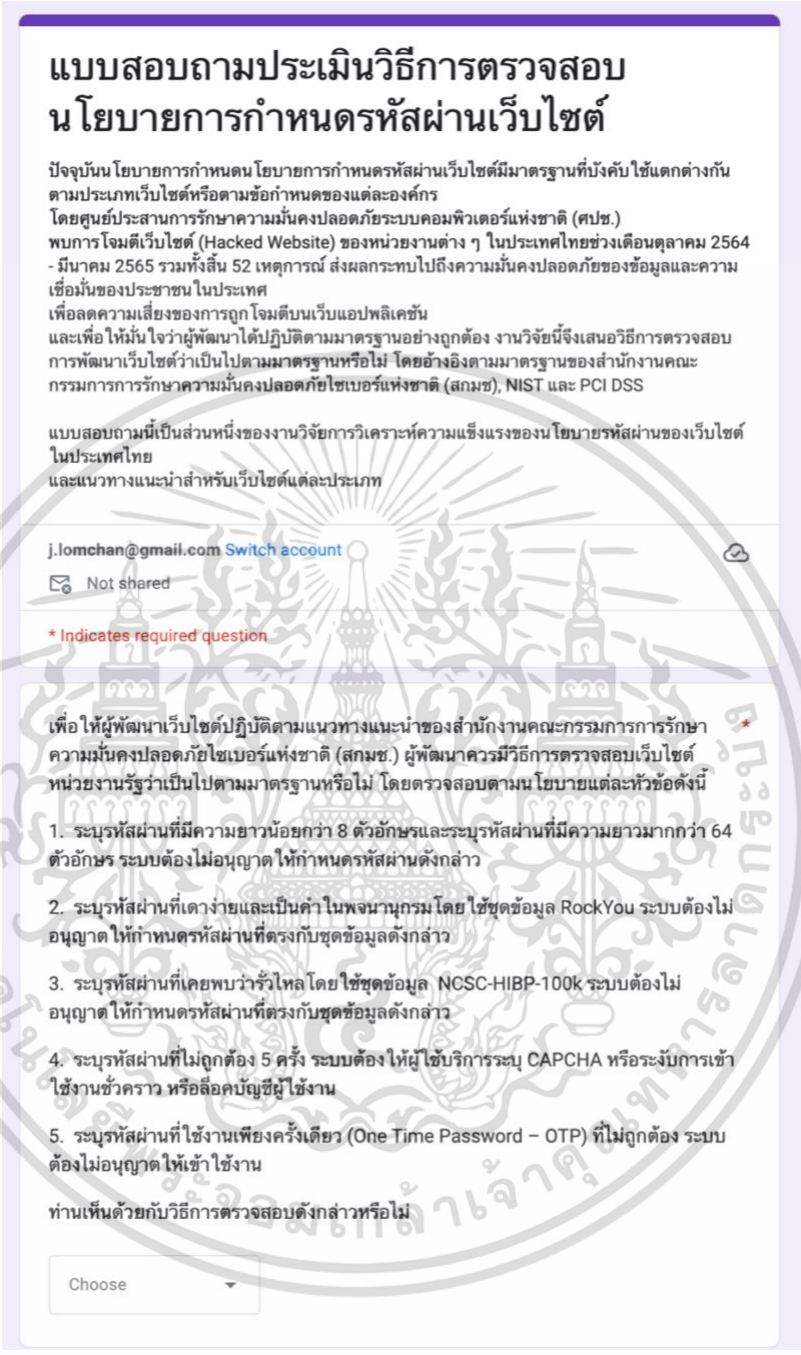
	1	2	3	4	5
Password ต้องยาวอย่างน้อย 7 ตัวอักษร ประกอบด้วยตัวเลขอย่างน้อยหนึ่งตัว และตัวอักษรภาษาอังกฤษอย่างน้อยหนึ่งตัว	○	○	○	○	○
ต้องเปลี่ยน password ทุก 90 วัน และต้องไม่ซ้ำกับ 4 password ที่เคยใช้งานก่อนหน้า	○	○	○	○	○
Password ต้องไม่ใช่ password ที่เคยพบว่าถูกละเมิดหรือรั่วไหล เช่น P@assw0rd, Qwertyuiop	○	○	○	○	○
Password ต้องไม่ใช่ password ที่เดาง่าย เช่น iloveyou	○	○	○	○	○
หากระบุ password ผิดหกครั้ง จะถูกระงับบัญชีเป็นเวลา 30 นาที หรือเมื่อผู้ดูแลระบบทำการปลดล็อก	○	○	○	○	○
ต้องใช้ Multi factor authentication ในการเข้าสู่ระบบ เช่น OTP, Google Authentication	○	○	○	○	○

หากต้องปฏิบัติตามนโยบายการกำหนดรหัสผ่านเว็บไซต์ทุกข้อข้างต้น เพื่อลดความเสี่ยงการเข้าถึงข้อมูลส่วนบุคคลที่ไม่ถูกต้อง ท่านเต็มใจที่จะปฏิบัติตามในระดับใด

Choose

Back Submit Clear form

2. แบบสอบถามประเมินวิธีการตรวจสอบนโยบายการกำหนดรหัสผ่านเว็บไซต์



แบบสอบถามประเมินวิธีการตรวจสอบนโยบายการกำหนดรหัสผ่านเว็บไซต์

ปัจจุบันนโยบายการกำหนดนโยบายการกำหนดรหัสผ่านเว็บไซต์มีมาตรฐานที่บังคับใช้แตกต่างกันตามประเภทเว็บไซต์หรือตามข้อกำหนดของแต่ละองค์กร
โดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.)
พบการโจมตีเว็บไซต์ (Hacked Website) ของหน่วยงานต่าง ๆ ในประเทศไทยช่วงเดือนตุลาคม 2564 - มีนาคม 2565 รวมทั้งสิ้น 52 เหตุการณ์ ส่งผลกระทบไปถึงความมั่นคงปลอดภัยของข้อมูลและความเชื่อมั่นของประชาชนในประเทศ
เพื่อลดความเสี่ยงของการถูกโจมตีบนเว็บแอปพลิเคชัน
และเพื่อให้มั่นใจว่าผู้พัฒนาได้ปฏิบัติตามมาตรฐานอย่างถูกต้อง งานวิจัยนี้จึงเสนอวิธีการตรวจสอบการพัฒนาเว็บไซต์ว่าเป็นไปตามมาตรฐานหรือไม่ โดยอ้างอิงตามมาตรฐานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช), NIST และ PCI DSS

แบบสอบถามนี้เป็นส่วนหนึ่งของงานวิจัยการวิเคราะห์ความแข็งแรงของนโยบายรหัสผ่านของเว็บไซต์ในประเทศไทย
และแนวทางแนะนำสำหรับเว็บไซต์แต่ละประเภท

j.lomchan@gmail.com Switch account

Not shared

* Indicates required question

เพื่อให้ผู้พัฒนาเว็บไซต์ปฏิบัติตามแนวทางแนะนำของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ผู้พัฒนาควรมีวิธีการตรวจสอบเว็บไซต์หน่วยงานรัฐว่าเป็นไปตามมาตรฐานหรือไม่ โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้ *

1. ระบุรหัสผ่านที่มีความยาวน้อยกว่า 8 ตัวอักษรและระบุรหัสผ่านที่มีความยาวมากกว่า 64 ตัวอักษร ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านดังกล่าว

2. ระบุรหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรมโดยใช้ชุดข้อมูล RockYou ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว

3. ระบุรหัสผ่านที่เคยพบว่ารั่วไหลโดยใช้ชุดข้อมูล NCSC-HIBP-100k ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว

4. ระบุรหัสผ่านที่ไม่ถูกต้อง 5 ครั้ง ระบบต้องให้ผู้ใช้บริการระบุ CAPCHA หรือระงับการเข้าใช้งานชั่วคราว หรือล็อคบัญชีผู้ใช้งาน

5. ระบุรหัสผ่านที่ใช้งานเพียงครั้งเดียว (One Time Password – OTP) ที่ไม่ถูกต้อง ระบบต้องไม่อนุญาตให้เข้าใช้งาน

ท่านเห็นด้วยกับวิธีการตรวจสอบดังกล่าวหรือไม่

Choose

หลังจากที่มีการบังคับใช้ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (Personal Data Protection Act) เพื่อให้องค์กรต่าง ๆ ที่มีการประมวลผลข้อมูลส่วนบุคคล ควรให้ความสำคัญกับการคุ้มครองข้อมูลส่วนบุคคล และพัฒนาระบบที่เกี่ยวข้องอย่างปลอดภัยและเป็นไปตามมาตรฐานสากล ซึ่งปัจจุบันยังไม่มีหน่วยงานใดกำหนดข้อบังคับที่ชัดเจน รวมถึงวิธีการตรวจสอบว่าปฏิบัติตามมาตรฐานหรือไม่ ผู้พัฒนาจึงควรมีวิธีการตรวจสอบเว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคลว่าเป็นไปตามมาตรฐาน NIST หรือไม่ โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้ *

โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้

1) ระบุรหัสผ่านที่มีความยาวน้อยกว่า 8 ตัวอักษรและระบุรหัสผ่านที่มีความยาวมากกว่า 64 ตัวอักษร ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านดังกล่าว

2) ระบุรหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันเกินสามตัวอักษรโดยใช้ชุดข้อมูล sequencePwd [?] ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่มีส่วนประกอบของรหัสผ่านตรงกับชุดข้อมูลดังกล่าว

3) ระบุรหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรมโดยใช้ชุดข้อมูล RockYou ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว

4) ระบุรหัสผ่านที่เคยพบว่ารั่วไหลโดยใช้ชุดข้อมูล NCSC-HIBP-100k ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว

5) ระบุรหัสผ่านที่ไม่ถูกต้อง 5 ครั้ง ระบบต้องให้ผู้ใช้บริการระบุ CAPCHA หรือระงับการเข้าใช้งานชั่วคราว หรือล็อคบัญชีผู้ใช้งาน

6) ระบุรหัสผ่านที่ใช้งานเพียงครั้งเดียว (One Time Password – OTP) ที่ไม่ถูกต้อง ระบบต้องไม่อนุญาตให้เข้าใช้งาน

ท่านเห็นด้วยกับวิธีการตรวจสอบดังกล่าวหรือไม่

Choose

ปัจจุบันการซื้อสินค้าและบริการผ่านเว็บไซต์เติบโตขึ้นมากในประเทศไทย บางระบบเสนอช่องทางการชำระเงินให้ผู้ใช้บริการสามารถเลือกใช้ได้ตามความสะดวก และยังสามารถเก็บข้อมูลการชำระเงินในระบบเพื่อใช้ในครั้งถัดไปได้ กรณีผู้ใช้งานเลือกชำระเงินผ่านช่องทางบัตรเครดิตและเก็บข้อมูลบัตรลงในระบบ จะมั่นใจได้อย่างไรว่าระบบมีความปลอดภัย เพื่อให้ผู้พัฒนาได้ตรวจสอบความปลอดภัยของระบบตนเองว่าได้พัฒนาส่วนของนโยบายการกำหนดรหัสผ่านตามมาตรฐานสากล ผู้พัฒนาจึงควรมีวิธีการตรวจสอบเว็บไซต์ที่มีการเก็บข้อมูลส่วนบุคคลว่าเป็นไปตามมาตรฐาน PCI DSS หรือไม่ โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้ *

โดยตรวจสอบตามนโยบายแต่ละหัวข้อดังนี้

1) ระบุรหัสผ่านที่มีความยาวน้อยกว่า 7 ตัวอักษรและต้องประกอบด้วยตัวเลขและตัวอักษรอย่างน้อยหนึ่งตัว หากไม่ตรงตามข้อกำหนด ระบบต้องไม่อนุญาตให้ใช้รหัสผ่านดังกล่าว

2) ระบุรหัสผ่านที่มีอักขระเดียวกันติดกันหรือเรียงลำดับกันเกินสามตัวอักษรโดยใช้ชุดข้อมูล sequencePwd ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่มีส่วนประกอบของรหัสผ่านตรงกับชุดข้อมูลดังกล่าว

3) ระบุรหัสผ่านที่เดาง่ายและเป็นคำในพจนานุกรมโดยใช้ชุดข้อมูล RockYou ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว

4) ระบุรหัสผ่านที่เคยพบว่ารั่วไหลโดยใช้ชุดข้อมูล NCSC-HIBP-100k ระบบต้องไม่อนุญาตให้กำหนดรหัสผ่านที่ตรงกับชุดข้อมูลดังกล่าว

5) ระบุรหัสผ่านที่ไม่ถูกต้อง 5 ครั้ง ระบบต้องให้ผู้ใช้บริการระบุ CAPCHA หรือระงับการเข้าใช้งานชั่วคราว หรือล็อคบัญชีผู้ใช้งาน

6) เข้าสู่เมนูเปลี่ยนรหัสผ่าน และทำการเปลี่ยนรหัสโดยใช้รหัสเดิมระบบต้องไม่อนุญาตให้ใช้รหัสผ่านดังกล่าว

7) เข้าสู่เมนูเปลี่ยนรหัสผ่าน และทำการเปลี่ยนรหัสโดยใช้รหัส 4 ครั้ง และทำการเปลี่ยนรหัสผ่านอีกครั้งโดยระบุรหัสผ่านที่กำหนดครั้งแรก ระบบต้องไม่อนุญาตให้ใช้รหัสผ่านดังกล่าว

8) ระบุรหัสผ่านที่ใช้งานเพียงครั้งเดียว (One Time Password – OTP) ที่ไม่ถูกต้อง ระบบต้องไม่อนุญาตให้เข้าใช้งาน

ท่านเห็นด้วยกับวิธีการตรวจสอบดังกล่าวหรือไม่

Choose

ท่านมีความเห็นหรือคำแนะนำเกี่ยวกับวิธีการตรวจสอบนโยบายการกำหนดรหัสผ่านที่เสนอหรือไม่

Your answer

Submit Clear form

ประวัติผู้เขียน

ชื่อ	นางสาวเจนจิรา ล้อมจันทร์
วัน เดือน ปีเกิด	27 เมษายน 2537
ที่อยู่ปัจจุบัน	33/1 หมู่ที่ 7 ตำบลเขาแหลม อำเภอชัยบาดาล จังหวัดลพบุรี 15130
ประวัติการศึกษา	สำเร็จการศึกษาระดับปริญญาตรีหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาการคอมพิวเตอร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง