ความสัมพันธ์แรงจูงใจในการป้องกันภัยและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ของประชาชน กรณีศึกษา: อำเภอจัตุรัส จังหวัดชัยภูมิ

วราภรณ์ ศรีบุญ[1] ประมุข ศรีชัยวงษ์ [2] และภานุวัฒน์ กิตติกรวรานนท์ รัตนพิมลพลแสน[3]

Retrieved 16-01-2026;
Revised 08-03-2026;
Accepted 27-03-2026

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ 1) เพื่อศึกษาเปรียบเทียบระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์จำแนกตามปัจจัยส่วนบุคคล 2) เพื่อศึกษาระดับแรงจูงใจในการป้องกันภัยจากมิจฉาชีพออนไลน์และระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ 3) เพื่อศึกษาความสัมพันธ์ระหว่างแรงจูงใจในการป้องกันภัยและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ โดยใช้การวิจัยเชิงสำรวจ ใช้ทฤษฎีแรงจูงใจป้องกันภัย และทฤษฎีการเผชิญปัญหา เป็นกรอบแนวคิดการวิจัย พื้นที่วิจัย คือ อำเภอจัตุรัส จังหวัดชัยภูมิ กลุ่มตัวอย่างคือประชาชนในอำเภอจัตุรัส จำนวน 383 คน ใช้การสุ่มแบบตามสะดวก ใช้แบบสอบถามในการเก็บรวบรวมข้อมูล และตรวจสอบคุณภาพของข้อมูล โดยการหาค่าความเที่ยงตรง การหาค่าอำนาจจำแนก และการหาค่าเชื่อมั่น วิเคราะห์ข้อมูลด้วยสถิติ ค่าร้อยละ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน t-test การวิเคราะห์ความแปรปรวนทางเดียว (One - way anova) และ Pearson Correlation Coefficient

ผลการวิจัย พบว่า 1) อายุ มีความแตกต่างมากที่สุด การศึกษา รองลงมา อาชีพ รองลงมาและรายได้ น้อยที่สุด มีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 ส่วนเพศไม่มีความแตกต่าง 2) ระดับแรงจูงใจในการป้องกันภัยพบว่า แรงจูงใจในการป้องกันภัยในภาพรวมอยู่ในระดับมาก โดยการรับรู้ความรุนแรงมากที่สุด รองลงมา ความคาดหวังในผลลัพธ์ในการปฏิบัติ รองลงมา การรับรู้ความเสี่ยงและ การรับรู้ความสามารถของตน และพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ในระดับภาพรวมอยู่ในระดับมาก โดยการหลีกเลี่ยงภัยมากที่สุด และรองลงมาการจัดการอารมณ์ 3) แรงจูงใจในการป้องกันมีความสัมพันธ์กับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 มีความสัมพันธ์ทางบวก (r= 0.79)

คำสำคัญ : แรงจูงใจป้องกันภัย,พฤติกรรมป้องกันภัย,มิจฉาชีพออนไลน์

ประเภทบทความ: บทความวิจัย

สังกัด[1]นักวิชาการอิสระ
ที่อยู่: 255 หมู่ 13 ตำบลบ้านกอก อำเภอจัตุรัส จังหวัดชัยภูมิ 36130
อีเมล์: warasri199@gmail.com
สังกัด[2] คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ
สังกัด[3] คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยภาคตะวันออกเฉียงเหนือ

The Relationship between Protection Motivation and Preventive Behaviors against Online Scammers among the Public: A Case Study of Chatturat District, Chaiyaphum Province

Waraporn Sribun[1] Pramuk Srichaiwong[2] Panuwat Kittikronwaranon Rattanapimonphonsaen[3]

Abstract

This research aimed to: 1) compare the level of preventive behaviors against online scammers classified by personal factors; 2) examine the level of protection motivation against online scammers and the level of preventive behaviors against online scammers; and 3) study the relationship between protection motivation and preventive behaviors against online scammers. This study employed a survey research design. Protection Motivation Theory and Coping Theory were used as the conceptual framework for the research. The research area was Chatturat District, Chaiyaphum Province. The sample consisted of 383 residents of Chatturat District, selected using convenience sampling. A questionnaire was used as the instrument for data collection. The quality of the instrument was examined through validity, discrimination power, and reliability tests. Data were analyzed using statistical methods including percentage, mean, standard deviation, t-test, one-way ANOVA, and Pearson Correlation Coefficient.

The results of the study revealed that: 1) Among personal factors, age showed the greatest difference, followed by education and occupation, while income showed the least difference. These differences were statistically significant at the 0.05 level. However, gender showed no significant difference. 2) The overall level of protection motivation was high. The highest aspect was perceived severity, followed by response efficacy, perceived risk, and self-efficacy. The overall level of preventive behaviors against online scammers was also high, with avoidance behavior being the highest, followed by emotional management. 3) Protection motivation was positively correlated with preventive behaviors against online scammers at a statistically significant level of 0.05, with a strong positive relationship (r = 0.79).

Keywords: Protection Motivation, Preventive Behaviors against, Online Scammers

Type of Article: Research Article

Affiliation[1] independent scholar
Address: 255 m00 13 bankok subdistrict,chatturat district,Chaiyaphum province
E-mail: warasri199@gmail.com
Affiliation[2] Faculty of social Sciences and Humanities,Northeastern University.
Affiliation[3] Faculty of social Sciences and Humanities,Northeastern University.

บทนำ

การเปลี่ยนผ่านสู่ดิจิทัล (Digital transformation) ได้ก่อให้การเปลี่ยนแปลง และสร้างแรงขับเคลื่อนในการเติบโต สร้างงาน และลดความยากจน ด้วยการนำเทคโนโลยีดิจิทัลมาใช้ในทุกส่วนขององค์การ มีการประเมินและปรับปรุงกระบวนการ ผลิตภัณฑ์ การดำเนินงาน และโครงสร้างเทคโนโลยีให้ทันสมัย รวดเร็ว เพื่อสร้างความสะดวกรวดเร็วใน การติดต่อสื่อสาร และการดำเนินงานต่างๆ ให้มีประสิทธิภาพมากยิ่งขึ้น โดยใช้เทคโนโลยีต่างๆ ในการดำเนินการ เช่นโครงสร้างพื้นฐานแบบไฮบริดคลาวด์ช่วยเพิ่มความยืดหยุ่น (Cloud Computing) รองรับธุรกรรมผ่านแอป (Mobile Technology) เป็นต้น ซึ่งการนำเทคโนโลยีได้ปรับเปลี่ยนพฤติกรรมประชาชนและ หน่วยงานต่างๆ ให้พึ่งพาเทคโนโลยีเพื่อใช้อำนวยความสะดวกให้รวดเร็วตอบสนองทันต่อความต้องการ แต่อย่างไรก็ตาม การเปลี่ยนผ่านสู่ดิจิทัล ได้สร้างความเสี่ยงให้แก่ผู้ใช้งาน สร้างความเสียหายและสูญเสียเนื่องจากมีกลุ่มบุคคลได้นำเทคโนโลยีนำมาปฏิบัติในการทำผิดกฎหมายโดยการใช้อุปกรณ์คอมพิวเตอร์ หรืออินเตอร์เน็ต สร้างความเสียหายให้แก่ประชาชน องค์การ ด้วยการใช้วิธีการต่างๆ เช่น การโจรกรรมข้อมูลส่วนตัวผ่านการสื่อสาร (Phishing) การเรียกค่าไถ่ของอาชญากรไซเบอร์ (Ransomware) เป็นต้น (สำนักงานที่ปรึกษาด้านการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ประจำสถานเอกอัครราชฑูต ณ กรุงวอชิงตัน,2568) ซึ่งการหลอกลวงได้สร้างความเสียหายให้แก่ประชาชน จึงนำไปสู่การหลอกลวงหลายรูปแบบ เช่น ในปี 2563 ในสหรัฐอเมริกา สำนักงานสอบสวนกลาง (Federal Bureau of Investigation: FBI รายงานการร้องเรียนเกี่ยวกับ อาชญากรรมทางคอมพิวเตอร์มีจำนวนถึง 7.9 แสนครั้ง เพิ่มขึ้นถึงร้อยละ 69 จากปี 2562 และมี มูลค่าความเสียหายรวมกว่า 4.2 พันล้านดอลลาร์สหรัฐ และ ในสหภาพยุโรป ผลสำรวจการหลอกลวง ทั้งจากออนไลน์และออฟไลน์ (scams and fraud) มีจำนวนตัวอย่างรวม 28,239 คน พบว่าร้อยละ 56 เคยมีประสบการณ์ถูกหลอกลวงอย่างน้อย 1 รูปแบบในรอบ 2 ปีที่ผ่านมา ซึ่งจากการสำรวจรูปแบบการหลอกลวงออกเป็น 3 รูปแบบหลัก 9 รูปแบบย่อย พบว่า การหลอกลวง ที่เกี่ยวข้องกับการเงิน/การให้ผลประโยชน์ (Monetary fraud) เป็นรูปแบบที่พบมากที่สุด รองลงมาคือ การโจรกรรมข้อมูลส่วนตัว (identity theft) และการหลอกลวงจากการซื้อขาย (buying scams) โดยคิดเป็น สัดส่วนร้อยละ 39 33 และ 23 ตามลำดับ (กองพัฒนาข้อมูลและตัวชี้วัดสังคม, 2565)

สำหรับประเทศไทย ประชาชนจำนวนมากได้ถูกหลอกลวงจากมิจฉาชีพ โดย ศูนย์ปฏิบัติการเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี (ศปอท) ได้รับแจ้งความเดือดร้อนจากประชาชน ซึ่งพบว่าผู้เสียหายจากสแกรมเมอร์ เป็นวัยทำงาน อายุ 20-49 ปี จำนวน 223,300 กรณี รองลงมา เป็นกลุ่มอายุ 50-64 ปี จำนวน 53,265 กรณี (เดลินิวส์,2586) โดยรูปแบบการหลอกลวง ได้แก่ 1) การส่ง sms line ปลอม แนบลิงค์เร่งให้ชำระหนี้ค่าปรับ 2) การหลอกลวงปลอมเสียงโทรศัพท์ วิดีโอปลอม ด้วยเทคโนโลยี AI 3) การหลอกลงทุนเงินคริปโต หุ้นดิจิทัล 4) สร้างโปรไฟล์ปลอมในแอปในโซเชียลหลอกลวงขายสินค้าปลอม หรือโรงแรมที่พักปลอม โดยใช้ช่องทางต่างๆ ได้แก่ 1) เฟซบุค จำนวน 126,672 กรณี มูลค่าความเสียหาย 2,810 ล้านบาท 2) คอลเซ็นเตอร์ (call center) จำนวน 32,000 กรณี มูลค่าความเสียหาย 2,660 ล้านบาท 3) เว็ปไซด์ จำนวน 10,000 กรณี มูลค่าความเสียหาย 1,710 ล้านบาท 4) ติ๊กต๊อก จำนวน 8,703 กรณี มูลค่าความเสียหาย 530 ล้านบาท โดยรูปแบบการหลอกลวง ได้แก่ 1) หลอกขอรหัสผ่านการใช้งานบัญชีอีเมล์ 2) แอบอ้างเป็นบุคคลต่าง ๆ หลอกจะโอนเงินหรือส่งของให้เหยื่อ 3) โฆษณาปล่อยเงินกู้นอกระบบมิจฉาชีพแอบอ้างเป็นผู้ให้บริการเงินกู้แล้วโฆษณาผ่านเว็บไซต์ต่าง ๆ หรือส่งอีเมลหาเหยื่อโดยตรง 4) ขอเลขที่บัญชีเงินฝากเป็นที่พักเงินมิจฉาชีพจะประกาศรับสมัครงานผ่านอินเทอร์เน็ต หลอกเหยื่อว่าเป็นบริษัทต่างประเทศที่ขายสินค้าในประเทศไทยเป็นจำนวนมาก จึงขอให้เหยื่อทำหน้าที่เป็นผู้รวบรวมเงินให้ โดยอาจจ่ายค่าจ้างเป็นสัดส่วนกับเงินที่ได้รับ เช่น ร้อยละ 25 ของเงินค่าสินค้า (ธนาคารแห่งประเทศไทย, มปป.)

อำเภอจัตุรัส เป็นอำเภอในจังหวัดชัยภูมิ ซึ่งประชาชนในอำเภอถูกหลอกลวงจากมิจฉาชีพออนไลน์หลายกรณี เช่น แอบอ้างเป็นตัวแทนจากกรมพัฒนาธุรกิจการค้าเพื่อติดต่อขอข้อมูลส่วนบุคคลจากผู้ประกอบธุรกิจและประชาชน ขอตรวจสอบข้อมูลธุรกิจต่างๆ หรือแอบอ้างมีโครงการกองทุนช่วยเหลือ SMEs ความช่วยเหลือผู้ประกอบธุรกิจที่ได้รับผลกระทบจาก โควิด -19 เป็นต้น โดยมิจฉาชีพจะติดต่อผ่านทางโทรศัพท์หรือส่งข้อความไปยังผู้ประกอบธุรกิจและประชาชนผ่านทางสื่อสังคมออนไลน์ (Social Media) ที่สร้างปลอมขึ้นมา เช่น Facebook หรือแอปพลิเคชัน Line หรือมีจดหมายส่งไปยังผู้ประกอบธุรกิจและประชาชน (องค์การบริหารส่วนตำบลละหาน,2565) 2) การร่อนใบปลิวเพื่อรับนักศึกษาเข้าทำงานกับธนาคารการเกษตรและสหกรณ์ โดยการสแกนคิวอาร์โคดเพื่อสมัครงาน (สำนักข่าวช่องวัน, 2565) 3) การหลอกลวงขายสินค้าแบรนด์เนม มูลค่า 3 ล้านบาท โดยการหลอกกดออร์เดอร์ ผ่านทางช่องไลน์ (สวพ.FM91, 2568) 4) การหลอกลวงประชาชนให้ชำระภาษีที่ดินและสิ่งลูกสร้างทางโทรศัพท์ในรูปแบบต่างๆ (องค์การบริหารส่วนตำบลหนองบัวบาน, 2566) เป็นต้น ซึ่งประชาชนได้รับความเดือดร้อนเสียหายจากการหลอกลวงของมิจฉาชีพ

การดำเนินการเพื่อป้องกันการถูกหลอกลวงจากมิจฉาชีพออนไลน์ในอำเภอจัตุรัสและในจังหวัดชัยภูมิมีความร่วมมือระหว่างสำนักงานตำรวจในจังหวัดชัยภูมิและกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม สร้างเครือข่ายนักล่าสแกรมเมอร์ ซึ่งดำเนินการภายใต้ยุทธการรู้ทันภัยไซเบอร์ เพื่อสร้างครูตำรวจต้นแบบ ซึ่งจะมีการอบรมตำรวจในสังกัด จำนวน 200 นายให้มีความเชี่ยวชาญด้านการโกงไซเบอร์ และมีเยาวชน จำนวน 30,000 คนเข้าร่วมโครงการ ซึ่งตำรวจที่ผ่านการอบรมจะเป็นวิทยากรให้ความรู้แก่นักเรียนมัธยมศึกษาใน 150 โรงเรียนภายในจังหวัดชัยภูมิเพื่อขยายผลต่อไปยังผู้ปกครองเป็นการป้องกันการถูกหลอกลวงจากมิจฉาชีพ (แนวหน้า, 2568)

พฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ มีแนวทางปฏิบัติเพื่อความปลอดภัย เช่น การปกป้องข้อมูลส่วนตัว การระมัดระวังในการใช้งาน เป็นต้น และแรงจูงใจในการป้องกันภัยจากมิจฉาชีพออนไลน์เป็นการป้องกันข้อมูลทรัพย์สิน ความปลอดภัย จากมิจฉาชีพ ซึ่งพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์และแรงจูงใจในการป้องกันภัยจากมิจฉาชีพออนไลน์ มีงานวิจัยที่ศึกษาถึงความสัมพันธ์ระหว่างตัวแปรพฤติกรรมการป้องกันภัยและแรงจูงใจป้องกันภัย เช่น งานวิจัยของ ศิริรัตน์ ศรีสว่าง (2558) พบว่าพฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์มีความสัมพันธ์กับความรู้ด้านความปลอดภัย และค่าใช้จ่ายในการป้องกัน สอดคล้อง กับธีรศักดิ์ พลพันธ์ (2564) พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเลกทรอนิกส์ได้รับอิทธิพลจากแรงจูงใจในการป้องกันการจัดการภัยคุกคาม อนุกูล นพคุณเจริญชัย (2561) การรับรู้ถึงจุดอ่อน การรับรู้ความรุนแรง ความเชื่อเกี่ยวกับอำนาจควบคุม การรับรู้ความสามารถของตนเอง การรับรู้ค่าใช้จ่ายจากการใช้เครื่องมือป้องกันภัยคุกคาม การรับรู้ประสิทธิผลในการปกป้องความเป็นส่วนตัว และแรงจูงใจในการเรียนรู้ทางสังคมส่งผลทางอ้อมต่อพฤติกรรมในการรับมือภัยคุก และนอกจากนี้ Liang and Xue (2009) ได้สร้างแบบจำลองการหลีกเลี่ยงภัยคุกคามทางเทคโนโลยี (Technology threat avoidance theory-TTAT) ได้ศึกษาถึงความสัมพันธ์ระหว่างแรงจูงใจในการป้องกันภัยและพฤติกรรมการป้องกันภัย โดยจากการทบทวนวรรณ พบว่ามีช่องว่างทางการศึกษา ซึ่งการศึกษาพฤติกรรมการป้องกันภัยได้ศึกษาเพียงอารมณ์ความกลัวเท่านั้น ยังมีความรู้สึกหรืออารมณ์อีกหลายประเภทที่ยังไม่ได้ศึกษา ดังนั้นผู้วิจัยจึงได้ศึกษา เพิ่มเติมในประเด็นเรื่องการจัดการอารมณ์ที่มาจากความโลภ ความหลงตัวเอง ความกดดัน ความรัก เพื่อศึกษาให้ครอบคลุมมากยิ่งขึ้น โดยศึกษาถึงความสัมพันธ์แรงจูงใจในการป้องกันภัยและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ซึ่งผลจากการศึกษาจะทำให้ทราบถึงแรงจูงใจในการป้องกันภัยและพฤติกรรมในการป้องกันภัยจากมิจฉาชีพออนไลน์ ซึ่งจะเป็นประโยชน์ต่อประชาชนในการป้องภัยที่มาจากมิจฉาชีพเพื่อเป็นการป้องกันการถูกหลอกลวง

วัตถุประสงค์การวิจัย

1. เพื่อศึกษาเปรียบเทียบระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์จำแนกตามปัจจัยส่วนบุคคล

2. เพื่อศึกษาระดับแรงจูงใจในการป้องกันภัยจากมิจฉาชีพออนไลน์และระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์

3. เพื่อศึกษาความสัมพันธ์ระหว่างแรงจูงใจในการป้องกันภัยและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์

สมมติฐานการวิจัย

1. ปัจจัยส่วนบุคคลแตกต่างกันพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์แตกต่างกัน

2. แรงจูงใจในการป้องกันมีความสัมพันธ์กับพฤติกรรมป้องกันจากมิจฉาชีพออนไลน์

การทบทวนวรรณกรรม

ทฤษฎีแรงจูงใจในการป้องกันภัย และพฤติกรรมป้องกันภัย โดยมีรายละเอียดดังนี้

ทฤษฎีแรงจูงใจในการป้องกันตนเอง (Protection Motivation Theory: PMT) เป็นทฤษฎีที่อธิบายผลกระทบของการสื่อสารเชิงโน้มน้าวใจต่อพฤติกรรมการป้องกันตนเอง โดยเน้นกลไกทางความคิดที่เป็นตัวกลางในการกระตุ้นความกลัวและการเปลี่ยนแปลงพฤติกรรม ทฤษฎีแรงจูงใจในการป้องกันตนเอง (Protection Motivation Theory: PMT) ถูกนำเสนอครั้งแรกโดย Rogers (1975) และได้รับการปรับปรุงเพิ่มเติมในปี ค.ศ. 1983 (Rogers, 1983) เพื่ออธิบายผลกระทบของการสื่อสารเชิงโน้มน้าวใจต่อพฤติกรรมการประเมินภัยคุกคาม (threat appraisal) ได้แก่ ความรุนแรง ความเสี่ยง และการประเมินการเผชิญปัญหา (coping appraisal) เป็นกระบวนการประเมินที่แตกต่างกัน ซึ่งนำไปสู่การตอบสนองทั้งแบบเชิงปรับตัว ได้แก่ ความคาดหวังในผลลัพธ์ ความเชื่อมั่นในความสามารถตน

Liang and Xue (2009) ได้พัฒนาแบบจำลอง โดยดัดแปลงมาจาก ทฤษฎีแรงจูงใจในการป้องกันภัยตนเอง โดยสร้างแบบจำลองการหลีกเลี่ยงภัยคุกคามทางเทคโนโลยี (Technology Threat Avoidance Theory - TTAT) โดยผู้ใช้จะปรับเปลี่ยนพฤติกรรมเพื่อหลีกเลี่ยงภัยคุกคามด้านข้อมูล โดยพิจารณาจาก การรับรู้ถึงภัยคุกคาม (Threat Perception) และ การรับรู้ถึงประสิทธิผลของมาตรการป้องกัน (Perceived Efficacy) ซึ่งนำไปสู่พฤติกรรมการหลีกเลี่ยง องค์ประกอบหลักของแบบจำลอง 1) การรับรู้ถึงภัยคุกคาม (Threat Perception) ผู้ใช้ประเมินว่าภัยคุกคามนั้นรุนแรงและมีความเป็นไปได้ระดับใด 2) การรับรู้ถึงประสิทธิผลของมาตรการป้องกัน (Perceived Efficacy) ผู้ใช้มีความเชื่อต่อมาตรการป้องกัน สามารถลดภัยคุกคามได้จริง 3) พฤติกรรมการหลีกเลี่ยง (Avoidance Behavior) หากภัยคุกคามสูงและมาตรการป้องกันได้ผล ผู้ใช้มีแนวโน้มที่จะหลีกเลี่ยงการใช้เทคโนโลยีหรือบริการนั้นๆ

Naqvi et al. (2024) องค์ประกอบต่าง ๆ ของการประเมินภัยคุกคาม (threat appraisal) การประเมินความสามารถในการรับมือ (coping appraisal) และการวิเคราะห์ต้นทุน-ผลประโยชน์ มีส่วนในการกำหนดการตัดสินใจของบุคคลในการนำพฤติกรรมด้านความปลอดภัยไซเบอร์มาใช้

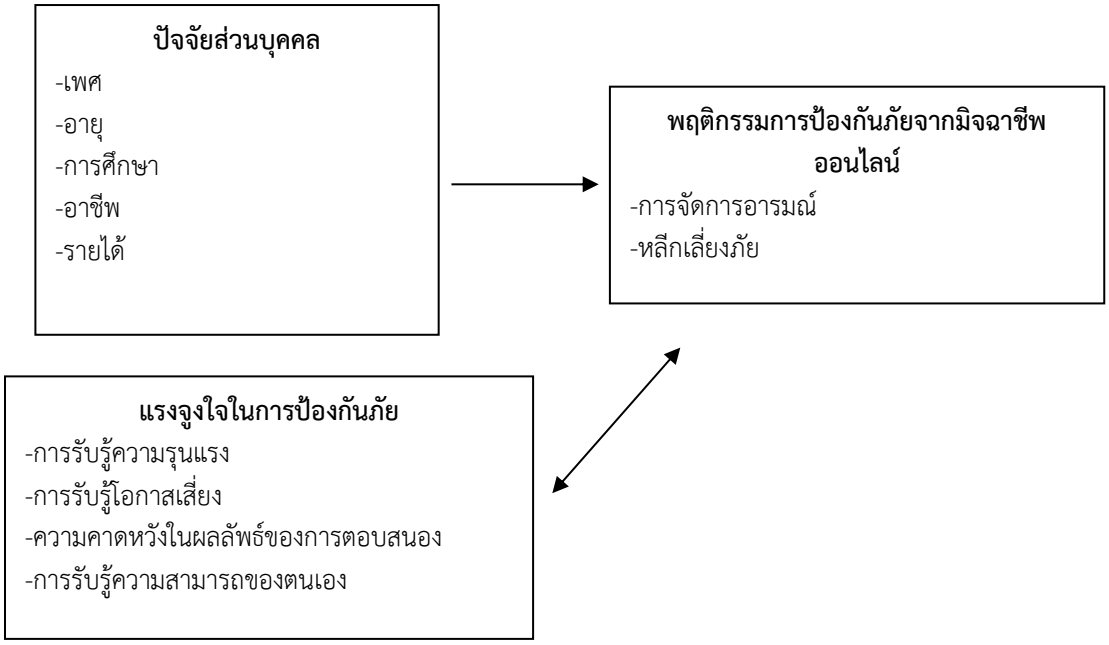
Duzenci , Kitapci and Gok. (2023) ผลการวิจัยพบว่า รูปแบบการตัดสินใจของบุคคลส่งผลต่อพฤติกรรมการปฏิบัติตามด้านความปลอดภัยไซเบอร์ และผลกระทบดังกล่าวมีความแตกต่างกันอย่างมีนัยสำคัญตามลักษณะรูปแบบการตัดสินใจของแต่ละบุคคลนอกจากนี้ ความตระหนักด้านความปลอดภัย (security awareness) เป็นตัวชี้วัดสำคัญของพฤติกรรมการปฏิบัติตามด้านความปลอดภัยไซเบอร์

Branley-Bell et al. (2022) ผลการวิจัยพบความแตกต่างด้านอายุอย่างมีนัยสำคัญ อย่างไรก็ตาม ความสัมพันธ์ดังกล่าวไม่ได้เป็นไปในทิศทางเดียวกันอย่างชัดเจน ผู้ใช้ที่มีอายุมากกว่ามีแนวโน้มตั้งค่าความปลอดภัยของอุปกรณ์น้อยกว่าผู้ใช้ที่อายุน้อยกว่า แต่ผู้ใช้ที่มีอายุมากกว่ากลับมีแนวโน้มมากกว่าที่จะสร้างรหัสผ่านที่ปลอดภัย มีความตระหนักรู้ถึงความเสี่ยงเชิงรุก และติดตั้งการอัปเดตอย่างสม่ำเสมอ เพศไม่ใช่ตัวทำนายที่มีนัยสำคัญของพฤติกรรมด้านความปลอดภัย (ผู้ชายจะมีคะแนนสูงกว่าในด้านการรับรู้ความสามารถด้านคอมพิวเตอร์ของตนเอง และความยืดหยุ่นโดยรวม) ซึ่งความเชื่อมั่นในความสามารถของตนเอง (self-efficacy) เป็นตัวแปรสื่อกลางระหว่างอายุและพฤติกรรมด้านความปลอดภัยไซเบอร์ 3 ด้าน ได้แก่ การสร้างรหัสผ่าน การตรวจสอบเชิงรุก และการอัปเดต นอกจากนี้ ความยืดหยุ่นโดยรวม (general resilience) เป็นตัวแปรสื่อกลางที่มีนัยสำคัญสำหรับการตั้งค่าความปลอดภัยของอุปกรณ์ การสร้างรหัสผ่าน และการอัปเดต อย่างไรก็ตาม ความยืดหยุ่นทำหน้าที่เป็นตัวแปรกำกับ (moderator) ของการตรวจสอบเชิงรุก

Sulaiman et al.(2022) ผลการวิจัยพบว่า พนักงานที่มีแรงจูงใจสูง และมีการรับรู้ระดับสูงเกี่ยวกับความรุนแรงของภัย (severity) ความเปราะบางหรือโอกาสเสี่ยง (vulnerability) ประสิทธิผลของการตอบสนอง (response efficacy) และความเชื่อมั่นในความสามารถของตนเอง (self-efficacy) จะมีพฤติกรรมการปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมมากขึ้น

กรอบแนวคิดการวิจัย

งานวิจัยนี้เป็นการวิจัยเชิงเชิงสำรวจ ผู้วิจัยกำหนดกรอบแนวคิดการวิจัยตามทฤษฎีแรงจูงใจในการป้องกันตนเองของ Rogers (1983) และแบบจำลอง Liang and Xue (2009) รวมถึงงานวิจัยของ Naqvi et al. (2024). Duzenci , Kitapci and Gok. (2023) Branley-Bell and (2022) จากการทบทวนทฤษฎีแรงจูงใจในการป้องกันตนเอง (Protection Motivation Theory: PMT) และแบบจำลอง ทฤษฎีแรงจูงใจในการป้องกันตนเอง และแบบจำลองการหลีกเลี่ยงการคุกคามทางเทคโนโลยี (Technology Threat Avoidance Theory - TTAT) ศึกษาเน้นอารมณ์ความกลัวเท่านั้น ยังไม่ศึกษาการจัดการอารมณ์ที่มาจากความโลภ ความหลงตัวเอง ความกดดัน ความรัก ดังนั้นงานวิจัยนี้จึงศึกษาการจัดการอารมณ์ เพิ่ม โดยนำทฤษฎีการเผชิญปัญหา (Coping Theory) ของ Lazarus and Folkman (1984) ซึ่งมีกลยุทธ์คือการเผชิญปัญหาโดยมุ่งเน้นที่ตัวปัญหา (Problem-Focused Coping) และการเผชิญปัญหาโดยมุ่งเน้นที่อารมณ์ (Emotion-Focused Coping) ซึ่งบุคคลจะประเมินสถานการณ์ (Appraisal) ก่อนจะเลือกกลยุทธ์ที่เหมาะสม เพื่อรักษาภาวะสมดุลทางจิตใจ โดยมีรายละเอียดดังนี้



ภาพที่ 1 กรอบแนวคิดในการวิจัย

ระเบียบวิธีวิจัย

งานวิจัยนี้เป็นงานวิจัยเชิงสำรวจ พื้นที่วิจัย คือ อำเภอจัตุรัส จังหวัดชัยภูมิ โดยมีการดำเนินการวิจัยดังนี้

1.ประชากรและกลุ่มตัวอย่าง

ประชากร คือ ผู้ที่มีอายุตั้งแต่ 16 ปี ถึงอายุ 79 ในอำเภอจัตุรัส จังหวัดชัยภูมิ จำนวน 45,071 คน (กระทรวงสาธารณสุข, 2569)

กลุ่มตัวอย่าง คือ ผู้ที่มีอายุตั้งแต่ 16 ปี ถึงอายุ 79 ปี ในอำเภอจัตุรัส จังหวัดชัยภูมิ ขนาดกลุ่มตัวอย่างกำหนดขนาดด้วยวิธีการของ Krejuice and morgan (1970) จำนวน 383 คน การสุ่มตัวอย่าง ใช้การสุ่มตัวอย่างแบบสะดวก (convenience sampling)

เครื่องมือในการวิจัย คือแบบสอบถาม จำนวน 3 ตอน ตอนที่ 1 ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม ตอนที่ 2 แบบวัดแรงจูงใจในการป้องกันภัยของประชาชน แบบมาตรวัด 5 ระดับ ของ likert scale ประกอบด้วย การรับรู้ความรุนแรง การรับรู้ความเสี่ยง ความคาดหวังในผลลัพธ์ของการปฏิบัติ การรับรู้ความสามารถตน โดยการคำนวณหาค่าความเชื่อมั่น ของครอนบาค ตอนที่ 3 แบบวัดพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ของประชาชน ด้วยมาตรวัด 5 ระดับ ของ likert ประกอบด้วย การจัดการอารมณ์ การหลีกเลี่ยงภัย

การตรวจสอบคุณภาพของข้อมูล โดยการหาค่าความเที่ยงตรง (content validity) ด้วยการหาค่าความสอดคล้อง (index of Item objective congruence : IOC) ตามเกณฑ์ Rovinelli และ Hambleton (1977) โดยข้อคำถามมีค่าตั้งแต่ 0.67 - 1.00 และการหาค่าอำนาจจำแนกด้วย item -total correlation มีค่าตั้งแต่ 0.55- 0.75 ตามเกณฑ์ Nunnally & Bernstein (1994) และการหาค่าเชื่อมั่น (reliability) ตามเกณฑ์ Cronbach (1951) โดยมีรายละเอียดดังนี้

ตาราง 1 การวิเคราะห์ค่าความเชื่อมั่น แบบสอบถาม โดยใช้ Cronbach ดังนี้

ตัวแปร	ค่าสัมประสิทธิ์
แรงจูงใจในการป้องกันภัย	0.95
การรับรู้ความรุนแรง	0.90
การรับรู้ความเสี่ยง	0.91
ความคาดหวังในผลลัพธ์ของการปฏิบัติ	0.87
การรับรู้ความสามารถตน	0.89
พฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์	0.92
การจัดการอารมณ์	0.86
การหลีกเลี่ยงภัย	0.90
แรงจูงใจในการป้องกันภัยและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์	0.96

การวิเคราะห์และสถิติที่ใช้

การวิเคราะห์

1. วิเคราะห์ปัจจัยส่วนบุคคล ใช้สถิติเชิงพรรณา ได้แก่ ร้อยละ ค่าเฉลี่ย

2. วิเคราะห์ระดับแรงจูงใจในการป้องกันภัยออนไลน์และระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ ใช้สถิติเชิงพรรณา ได้แก่ ค่าความถี่และ ส่วนเบี่ยงเบนมาตรฐาน

3. วิเคราะห์เปรียบเทียบจำแนกตามปัจจัยส่วนบุคคลโดย ใช้ t -test สำหรับ 2 กลุ่มประชากร และวิเคราะห์ความแปรปรวนทางเดียว (one-way anova) สำหรับประชากรที่มีมากกว่า 2 กลุ่มขึ้นไป

4. การศึกษาเพื่อวิเคราะห์ความสัมพันธ์แรงจูงใจในการป้องกันภัยออนไลน์กับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ ใช้ Pearson Correlation Coefficient

ผลการวิจัย

วัตถุประสงค์ที่ 1 เพื่อศึกษาระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์จำแนกตามปัจจัยส่วนบุคคล ผลการศึกษาพบว่า

ผลการศึกษาปัจจัยส่วนบุคคล ได้แก่ เพศ อายุ การศึกษา อาชีพ รายได้ ดังนี้

1. เพศ จากการศึกษา พบว่า ผู้ตอบแบบสอบถามจำนวน 383 คน เป็นชายจำนวน 165 คน ร้อยละ 43.1 และ เป็นหญิง 218 คน ร้อยละ 56.9 ผู้ตอบส่วนใหญ่เป็นเพศหญิงร้อยละ 56.9

2. อายุ จากการศึกษา พบว่า อายุ 16-28 มากที่สุด จำนวน 102 คน ร้อยละ 26.6 รองลงมา อายุ 45-60 และ 61-79 จำนวน 94 คน ร้อยละ 24.5 และอายุ 29-44 น้อยที่สุด จำนวน 93 คน ร้อยละ 24.3

3. การศึกษา จากการศึกษา พบว่า ระดับมัธยมศึกษา มากที่สุด จำนวน 127 คน ร้อยละ 33.2 รองลงมา ประถมศึกษา จำนวน 105 คน ร้อยละ 27.4 และระดับประกาศนียบัตรวิชาชีพและสูงกว่าปริญญาตรี น้อยที่สุด จำนวน 23 คน ร้อยละ 6

4. อาชีพ จากการศึกษา พบว่า เกษตรกรมากที่สุด จำนวน 137 คน ร้อยละ 35.8 รองลงมาค้าขาย จำนวน 63 คน ร้อยละ 16.4 และพนักงานราชการน้อยที่สุด จำนวน 16 คน ร้อยละ 4.2

5. รายได้ จากการศึกษา พบว่า รายได้ต่ำกว่า 10,000 บาท มากที่สุด จำนวน 196 คน ร้อยละ 51.2 รองลงมา รายได้ 10,000-15,000 บาท จำนวน 89 คน ร้อยละ 23.2 และ รายได้ 15,000-20,000 และ 20,000 ขึ้นไปน้อยที่สุด จำนวน 49 คน ร้อยละ 12.8

ตาราง 2 การวิเคราะห์เปรียบเทียบปัจจัยส่วนบุคคลและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์

ปัจจัยส่วนบุคคล	t/F	Sig	แปลผล
เพศ	-1.612	0.11	ไม่แตกต่าง
อายุ	20.85	0.00	แตกต่าง
การศึกษา	15.59	0.00	แตกต่าง
อาชีพ	8.82	0.00	แตกต่าง
รายได้	5.17	0.00	แตกต่าง

จากผลการศึกษา ปัจจัยส่วนบุคคลกับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ ดังนี้

1) ปัจจัยส่วนบุคคล ดังนี้ 1.1) เพศแตกต่างกัน พบว่า เพศกับการพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ไม่แตกต่างกัน 1.2) อายุที่แตกต่างกันมีระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์มีความแตกต่างกัน อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 1.3) การศึกษาที่แตกต่างกันมีระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 1.4) อาชีพที่แตกต่างกันมีระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ที่แตกต่างกัน อย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 1.5) รายได้ที่แตกต่างกันมีระดับพฤติกรรมป้องกันภัยจากมิจฉาชีพออนไลน์ที่แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

ดังนั้นจากสมมติฐานที่ 1 ปัจจัยส่วนบุคคลแตกต่างกันพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์แตกต่างกัน โดย อายุ การศึกษา อาชีพ รายได้ มีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 และเพศไม่มีความแตกต่างกัน

วัตถุประสงค์ที่ 2 เพื่อศึกษาระดับแรงจูงใจในการป้องกันภัยจากมิจฉาชีพออนไลน์และระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ ผลการศึกษาพบว่า

ตาราง 3 ระดับแรงจูงใจในการป้องกันภัยและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์

ตัวแปร	$\bar{x}$	S.D.	ระดับ
แรงจูงใจในการป้องกันภัย	3.95	0.78	มาก
การรับรู้ความรุนแรง	4.13	0.86	มาก
การรับรู้ถึงความเสี่ยง	3.83	0.95	มาก
ความคาดหวังในผลลัพธ์ของการปฏิบัติ	4.10	0.77	มาก
การรับรู้ความสามารถตน	3.76	1.02	มาก
พฤติกรรมการป้องกันจากมิจฉาชีพออนไลน์	3.91	0.83	มาก
การจัดการอารมณ์	3.88	0.83	มาก
การหลีกเลี่ยงภัย	3.94	0.96	มาก

การวิเคราะห์แรงจูงใจในการป้องกันในภาพรวม มี ($\bar{X}$ = 3.95, S.D.= 0.78) ในระดับมาก โดยการรับรู้ความรุนแรง ($\bar{X}$ = 4.13, S.D. =0.86) ในระดับมาก การรับรู้ความเสี่ยง ($\bar{X}$ = 3.83, S.D.= 0.95) ในระดับมาก ความคาดหวังในผลลัพธ์การปฏิบัติ ($\bar{X}$= 4.10, S.D. = 0.77) ในระดับมาก การรับรู้ความสามารถของตน ($\bar{X}$ = 3.76, S.D. = 1.02) ในระดับมาก พบว่า การรับรู้ความรุนแรงมากที่สุด รองลงมา ความคาดหวังในผลลัพธ์ในการปฏิบัติ รองลงมา การรับรู้ความเสี่ยงและ การรับรู้ความสามารถของตน

การวิเคราะห์ระดับพฤติกรรมในการป้องกันภัย ในภาพรวม ($\bar{X}$ = 3.91, S.D. = 0.83) ในระดับมาก โดยการหลีกเลี่ยงภัย ($\bar{X}$ = 3.94, S.D. = 0.96) ในระดับมาก และ การจัดการอารมณ์ ($\bar{X}$ = 3.88, S.D. = 0.96) ในระดับมาก พบว่า การหลีกเลี่ยงภัยมากที่สุด และการจัดการอารมณ์รองลงมา

วัตถุประสงค์ที่ 3 เพื่อศึกษาความสัมพันธ์ระหว่างแรงจูงใจในการป้องกันภัยและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ ผลการวิจัยพบว่า

ตาราง 4 ความสัมพันธ์ระหว่างแรงจูงใจในการป้องกันภัย กับ พฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์

ตัวแปร	R	sig	การแปลผล
แรงจูงใจในการป้องกันภัย	0.79	0.00	ปานกลาง
การรับรู้ความรุนแรง	0.76	0.00	ปานกลาง
การรับรู้ถึงความเสี่ยง	0.65	0.00	ปานกลาง
ความคาดหวังในผลลัพธ์ของการปฏิบัติ	0.68	0.00	ปานกลาง
การรับรู้ความสามารถของตน	0.64	0.00	ปานกลาง

จากการศึกษา พบว่า แรงจูงใจในการป้องกันมีความสัมพันธ์กับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดย มีความสัมพันธ์ทางบวก (r= 0.79)

ความสัมพันธ์ระหว่างพฤติกรรมป้องกันภัยจากมิจฉาชีพออนไลน์ และด้านต่างๆ ของแรงจูงใจในการป้องกันภัย พบว่า มีความสัมพันธ์กันทางบวกกับแรงจูงใจทุกด้าน โดยมีความสัมพันธ์กับ การรับรู้ความรุนแรงมากที่สุด (r= 0.76) รองลงมา ความคาดหวังในผลลัพธ์ของการปฏิบัติ (r=0.68) รองลงมา การรับรู้ความเสี่ยง (r= 0.65) และ การรับรู้ความสามารถตน (r= 0.64) อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

ดังนั้นจากสมมติฐานที่ 2 แรงจูงใจในการป้องกันมีความสัมพันธ์กับพฤติกรรมป้องกันจากมิจฉาชีพออนไลน์ โดยมีความสัมพันธ์ทางบวก อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 (r= 0.79) ซึ่งมีความสัมพันธ์ในระดับปานกลาง

อภิปรายผลการวิจัย

ผลจากการวิจัยวัตถุประสงค์ที่ 1 พบว่า พฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์จำแนกตามปัจจัยส่วนบุคคล พบว่า อายุ การศึกษา อาชีพ รายได้ ที่แตกต่างกันมีพฤติกรรมในการป้องกันภัยจากมิจฉาชีพออนไลน์ที่แตกต่างกัน และ เพศที่แตกต่างกันไม่มีความแตกต่างในพฤติกรรมการป้องกันภัยจาก

มิจฉาชีพออนไลน์ เนื่องจากพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ขึ้นอยู่กับ อายุ การศึกษา อาชีพ รายได้ สอดคล้องกับ Branley-Bell et al. (2022) พบความแตกต่างด้านอายุอย่างมีนัยสำคัญ อย่างไรก็ตาม ความสัมพันธ์ดังกล่าวไม่ได้เป็นไปในทิศทางเดียวกันอย่างชัดเจน ผู้ใช้ที่มีอายุมากกว่ามีแนวโน้มตั้งค่าความปลอดภัยของอุปกรณ์น้อยกว่าผู้ใช้ที่อายุน้อยกว่า แต่ผู้ใช้ที่มีอายุมากกว่ากลับมีแนวโน้มมากกว่าที่จะ สร้างรหัสผ่านที่ปลอดภัย มีความตระหนักรู้ถึงความเสี่ยงเชิงรุก และติดตั้งการอัปเดตอย่างสม่ำเสมอ เพศไม่ใช่ตัวทำนายที่มีนัยสำคัญของพฤติกรรมด้านความปลอดภัย (ผู้ชายจะมีคะแนนสูงกว่าในด้านการรับรู้ความสามารถด้านคอมพิวเตอร์ของตนเอง และความยืดหยุ่นโดยรวม) สอดคล้องกับสุธาเทพ รุณเรศ (2561) ปัจจัยทางด้านลักษณะทางประชากรด้านอายุ ระดับการศึกษาสูงสุด และรายได้ส่วนตัวต่อเดือน มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต แต่ปัจจัย ทางด้านลักษณะทางประชากรด้านเพศ ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

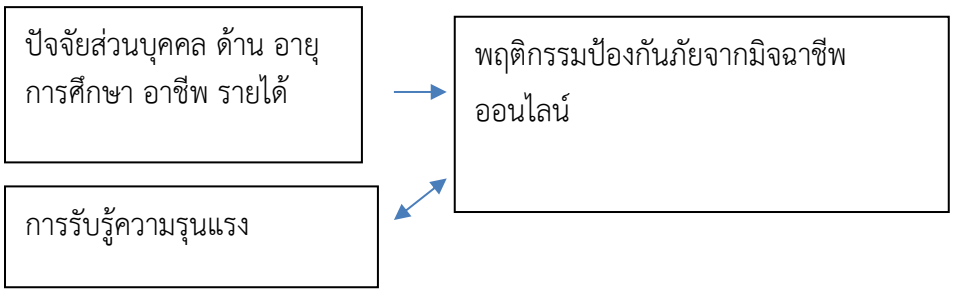
ผลจากการวิจัยวัตถุประสงค์ที่ 2 พบว่า ระดับแรงจูงใจในการป้องกันภัยจากมิจฉาชีพออนไลน์และระดับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ พบว่า แรงจูงใจในการป้องกันภัยในภาพรวมอยู่ในระดับมาก โดยการรับรู้ความรุนแรงค่าเฉลี่ยมากที่สุด รองลงมา ความคาดหวังในผลลัพธ์ในการปฏิบัติ รองลงมา การรับรู้ความเสี่ยงและ การรับรู้ความสามารถของตนค่าเฉลี่ยน้อยที่สุด และพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ในระดับภาพรวมอยู่ในระดับมาก โดยการหลีกเลี่ยงภัยค่าเฉลี่ยมากที่สุด และการจัดการอารมณ์ค่าเฉลี่ยรองลงมา สอดคล้องกับ Rogers (1983) แรงจูงใจในการป้องกันภัยมาจากผลกระทบของการสื่อสารเชิงโน้มน้าวใจต่อพฤติกรรมการประเมินภัยคุกคาม (threat appraisal) ได้แก่ ความรุนแรง ความเสี่ยงและการประเมินการเผชิญปัญหา (coping appraisal) เป็นกระบวนการประเมินที่แตกต่างกัน ซึ่งนำไปสู่การตอบสนองทั้งแบบเชิงปรับตัว ได้แก่ ความคาดหวังในผลลัพธ์ ความเชื่อมั่นในความสามารถตน และสอดคล้อง Sulaiman et al.(2022) พบว่า พนักงานที่มีแรงจูงใจสูง และมีการรับรู้ระดับสูงเกี่ยวกับความรุนแรงของภัย (severity) ความเปราะบางหรือโอกาสเสี่ยง (vulnerability) ประสิทธิผลของการตอบสนอง (response efficacy) และความเชื่อมั่นในความสามารถของตนเอง (self-efficacy) จะมีพฤติกรรมการปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสมมากขึ้น

ผลจากการวิจัยวัตถุประสงค์ที่ 3 พบว่า ความสัมพันธ์ระหว่างแรงจูงใจในการป้องกันภัยและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ พบว่า แรงจูงใจในการป้องกันมีความสัมพันธ์กับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยมีความสัมพันธ์ทางบวก (r= 0.79) ซึ่งแรงจูงใจป้องกันภัยที่มาจากการรับรู้ความรุนแรง การรับรู้ถึงความเสี่ยง ความคาดหวังในผลลัพธ์ของการปฏิบัติ การรับรู้ความสามารถของตน จะแสดงพฤติกรรมการป้องกันภัย ได้แก่ หลีกเลี่ยงภัย และการจัดการอารมณ์ สอดคล้องกับ ศิริรัตน์ ศรีสว่าง (2558) พฤติกรรมการป้องกันอาชญากรรมคอมพิวเตอร์ได้รับอิทธิพลจาก ปัจจัยส่วนบุคคล ได้แก่ บุคลิกภาพแบบมีจิตสำนึก การรับรู้คุณค่าของข้อมูล และประสบการณ์ในอดีต รวมทั้งปัจจัยด้านสภาพแวดล้อม ได้แก่ การคล้อยตามกลุ่มอ้างอิง ความรู้ด้านความปลอดภัย และค่าใช้จ่ายในการป้องกัน โดยส่งผ่านการรับรู้ต่อสภาวะคุกคาม การรับรู้ความสามารถในการ จัดการกับภัยคุกคาม และ แรงจูงใจในการป้องกัน สอดคล้องกับ ธีรศักดิ์ พลพันธ์ (2564) พบว่า พฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนบริการธุรกรรมทางอิเลคทรอนิกส์ได้รับอิทธิพลทางบวกโดยตรงจากความตั้งใจปกป้องข้อมูล และได้รับอิทธิพลทางบวกโดยอ้อมจากการรับรู้ถึงโอกาสเสี่ยงบนธุรกรรมทางอิเลคทรอนิกส์ ความคาดหวังความสามารถของตนเองในการปกป้องข้อมูลส่วนบุคคล สอดคล้องกับ Liang and Xue (2009) พบว่า ผู้ใช้จะมีแรงจูงใจในการหลีกเลี่ยงเทคโนโลยีที่เป็นอันตรายเมื่อพวกเขารับรู้ถึงภัยคุกคาม และเชื่อว่าภัยคุกคามนั้นสามารถหลีกเลี่ยงได้ด้วยการใช้มาตรการป้องกัน อย่างไรก็ตาม หากผู้ใช้เชื่อว่าภัยคุกคามไม่สามารถ

หลีกเลี่ยงได้อย่างสมบูรณ์ด้วยมาตรการดังกล่าว พวกเขาจะกลับไปใช้การเผชิญปัญหาแบบมุ่งเน้นอารมณ์ (emotion-focused coping) แทน

องค์ความรู้ใหม่จากการวิจัย

อายุ การศึกษา อาชีพ รายได้ ที่แตกต่างกันพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์แตกต่างกัน และแรงจูงใจในการป้องกันภัยด้านการรับรู้ความรุนแรงมีความสัมพันธ์กับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์มากที่สุด



สรุป

1. อายุ การศึกษา อาชีพ รายได้ ที่แตกแตกต่างกัน พฤติกรรมในการป้องกันภัยจากมิจฉาชีพออนไลน์ที่แตกต่างกัน และ เพศที่แตกต่างกันไม่มีความแตกต่างในพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์

2. แรงจูงใจในการป้องกันภัยในภาพรวมอยู่ในระดับมากและพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ในระดับภาพรวมอยู่ในระดับมาก

3. แรงจูงใจในการป้องกันมีความสัมพันธ์กับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดย มีความสัมพันธ์ทางบวก (r= 0.79)

ข้อเสนอแนะ

1. ข้อเสนอแนะในการนำผลการวิจัยไปใช้ประโยชน์

ผลจากการวิจัยวัตถุประสงค์ที่ 1 พบว่า อายุ การศึกษา อาชีพ รายได้ที่แตกต่างกัน พฤติกรรมการป้องกันภัยแตกต่างกัน หน่วยงานที่เกี่ยวข้องกับการส่งเสริมให้ความรู้ เพื่อหาทางป้องกันควบคุมควรให้ความสนใจ ด้าน อายุ การศึกษา อาชีพ รายได้

ผลจากการวิจัยวัตถุประสงค์ที่ 2 พบว่า แรงจูงใจในภาพรวมอยู่ในระดับมาก และพฤติกรรมการป้องกันภัยในภาพรวมอยู่ในระดับมาก ดังนั้น หน่วยงานที่เกี่ยวข้องจึงควรสนับสนุนการให้ความรู้เพื่อเป็นการป้องกันภัยจากมิจฉาชีพออนไลน์

ผลจากการวิจัยวัตถุประสงค์ที่ 3 พบว่าแรงจูงใจในการป้องกันมีความสัมพันธ์กับพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ หน่วยงานที่เกี่ยวข้องควรส่งเสริมให้ประชาชนมีแรงจูงใจในการป้องกันภัย ซึ่งจะสามารถลดการถูกหลอกลวงของประชาชนจากมิจฉาชีพออนไลน์ได้

2. ข้อเสนอแนะในการทำวิจัยครั้งต่อไป

งานวิจัยนี้ได้ข้อค้นพบ อายุ การศึกษา อาชีพ รายได้ ที่แตกต่างกัน พฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์มีความแตกต่างกัน ส่วนเพศที่แตกต่างกัน ไม่มีความแตกต่างต่อพฤติกรรมการป้องกันภัยจากมิจฉาชีพออนไลน์ และแรงจูงใจในการป้องกันภัยด้านการรับรู้รุนแรงมีความสัมพันธ์กับพฤติกรรมการป้องกัน

ภัยจากมิจฉาชีพออนไลน์มากที่สุด สามารถนำไปประยุกต์ใช้กับการรณรงค์เพื่อส่งเสริมการป้องกันการถูกหลอกลวงจากมิจฉาชีพออนไลน์ โดยควรให้ความสำคัญกับ อายุ การศึกษา อาชีพ รายได้ และการให้ความรู้ถึงความรุนแรงของการถูกหลอกลวงจากมิจฉาชีพมีผลเสียหายอย่างไร และมีผลกระทบอย่างไรบ้าง และในการวิจัยครั้งต่อไปควรทำวิจัยในประเด็นเกี่ยวกับ นโยบายการส่งเสริมการป้องกันภัยจากมิจฉาชีพออนไลน์

เอกสารอ้างอิง

กระทรวงสาธารณสุข. (2569). *ประชากรทะเบียนราษฎร์ วัยทำงาน (อายุ 15-59 ปี) ปีงบประมาณ 2566 ชัยภูมิ*. สืบค้นวันที่ 1 พฤศจิกายน 2568, จาก https://dashboard.anamai.moph.go.th/population/pop-workingage/changwat?year=2023&cw=36.

กองพัฒนาข้อมูลและตัวชี้วัดสังคม. (2565). *สภาพปัญหาการหลอกลวงยุคดิจิทัล และแนวทางแก้ไข*. สืบค้นวันที่ 1 พฤศจิกายน 2568, จาก https://www.nesdc.go.th/wordpress/wp-content/uploads/2025/06/2565_article_q1_003.pdf.

เดลินิวส์. (31 ธันวาคม 2568) *เปิด 4 เทรนด์สแกมเมอร์ ปี 69 เตือนภัย ปชช. ต้องรู้ทันกลโกงของมิจฉาชีพ!!* . สืบค้นเมื่อ 31 ธันวาคม 2568, จาก https://www.dailynews.co.th/news/5458599/.

ธนาคารแห่งประเทศไทย. (ม.ป.ป.). *กลโกงออนไลน์อื่นๆ*. สืบค้นเมื่อ 10 พฤศจิกายน 2568 จาก, https://www.bot.or.th/th/satang-story/fraud/online-crime.html.

นิธิป ชวนตันติกมล. (2557). *พฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัว ภายใน Public Cloud*. (วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต). คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์.

แนวหน้า. (24 พฤศจิกายน 2568) .*ตำรวจชัยภูมิ'สร้างเครือข่ายนักล่า'สแกมเมอร์' ดึงเยาวชน 3 หมื่นคนร่วมทัพต้านโกงออนไลน์*.สืบค้นเมื่อ 1 ธันวาคม 2568, จาก https://www.naewna.com/local/930023.

ธีรศักดิ์ พลพันธ์. (2564). *ปัจจัยเชิงเหตุของพฤติกรรมการปกป้องข้อมูลส่วนบุคคลบนธุรกรรมทางอิเลคทรอนิกสในกลุ่มวัยทำงานตอนต้น. (*ปรัชญาดุษฎีบัณฑิต). บัณฑิตวิทยาลัย มหาวิทยาลัยศรีนครินทรวิโรฒ.

สวพ.FM91. (21 พฤษภาคม 2568) . *รวบแก๊งบัญชีม้า หลอกกดออเดอร์ ขายกระเป๋าแบรนด์เนม สูญเงินกว่า 3 ล้านบาท.* สืบค้นเมื่อ 20 พฤศจิกายน 2568, จาก https://today.line.me/th/v3/article/oqml6Py.

สำนักข่าวช่องวัน. (2 สิงหาคม 2565). *มุกใหม่มิจฉาชีพ ร่อนใบปลิวรับนักศึกษาฯ สแกนคิวอาร์โค้ดสมัครงาน หลอกเอาข้อมูล*. สืบค้นเมื่อ 10 พฤศจิกายน 2568, จาก https://www.one31.net/news/detail/56856.

สำนักงานจังหวัดชัยภูมิ. (1 พฤษภาคม 2568). *ประชากรและโครงสร้างประชากร.* จาก https://www.chaiyaphum.go.th/page_about/about2.1.php.

สำนักงานที่ปรึกษาด้านการอุดมศึกษา วิทยาศาสตร์ วิจัยและนวัตกรรม ประจำสถานเอกอัครราชฑูต ณ กรุงวอชิงตัน. (30 ธันวาคม 2568). Cybercrime ผลกระทบต่อความมั่นคงของสังคมดิจิทัล. สืบค้นเมื่อ 1 มีนาคม 2569, จาก https://www.ohesdc.org/post/cybercrime.

สุธาเทพ รุณเรศ. (2561) . *ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร.*(วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต). วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์.

ศิริรัตน์ ศรีสว่าง. (2558).*ปัจจัยที่ส่งผลต่อพฤติกรรมการป้องกันภัยจากอาชญากรรมคอมพิวเตอร์ของผู้ใช้คอมพิวเตอร์.*(วิทยานิพนธ์วิทยาศาสตรมหาบัณฑิต). คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์.

องค์การบริหารส่วนตำบลละหาร. (14 ธันวาคม 2565). *ประชาสัมพันธ์เตือนผู้ประกอบธุรกิจและประชาชนอย่าหลงเชื่อกลุ่มมิจฉาชีพ*. สืบค้นเมื่อ 20 พฤศจิกายน 2568, จาก https://www.tumbonlahan.go.th/select_news.php?news_id=5297.

องค์การบริหารส่วนตำบลหนองบัวบาน. (19 มิถุนายน 2566). *ขอความอนุเคราะห์ปิดประกาศและประชาสัมพันธ์ประกาศหอกระจายข่าว*. สืบค้นเมื่อ 20 พฤศจิกายน 2568, จาก https://nongbuaban.go.th/fileupload/5015668743.pdf.

อนุกูล นพคุณ เจริญชัย. (2561). *ปัจจัยที่กำหนดพฤติกรรมในการรับมือกับภัยคุกคามทางคอมพิวเตอร์ต่อการสูญเสียและถูกโจรกรรมข้อมูลทางการเงิน: กรณีศึกษาโปรแกรมทางการบัญชีสำหรับธุรกิจขนาดเล็ก*. (วิทยานิพนธ์บัญชีมหาบัณฑิต). คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์.

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). *Exploring age and gender differences in ICT cybersecurity behaviour*. Human Behavior and Emerging Technologies*, 2022*.https://doi.org/10.1155/2022/2693080

Cronbach, L. J. (1951). *Coefficient alpha and the internal structure of tests.* Psychometrika, 16(3), 297–334.

Duzenci, A., Kitapci, H., & Gok, M. S. (2023). *The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior*. Applied Sciences*, 13*(15), 8731. https://doi.org/10.3390/app13158731

Krejcie, R. & Morgan, D. (1970). *Determining sample sizes for research activities*.Educational and Psychological Measurement 30: 607-610.

Lazarus, R. S., & Folkman, S. (1984). *Stress, Appraisal, and Coping*. Springer Publishing.

Liang, H., & Xue, Y. (2009). *Avoidance of Information technology threats: a therotical perspective*. MIS Quarterly, 33(1), 71-90.

Naqvi, S. G., Alishba, Mughal, M. A., Shehzad, K., & Noor, R. T. (2024). *Organizational environment, protection motives, adoption of machine learning, and cybersecurity behavior*. Journal of Excellence in Social Sciences, 3(4), 11–25.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3rd ed.). McGraw-Hill.

Rogers, R.W. (1983). *Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation*. In J. Cacioppo & R. Petty (Eds.), Social Psychophysiology. New York: Guilford Press.

Rovinelli, R. J., & Hambleton, R. K. (1977). *On the use of content specialists in the assessment of criterion-referenced test item validity*. Dutch Journal of Educational Research.

Sulaiman, N.S., Fauzi, M.A., Hussain, S., Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks.Information, 13(413),1-17.