การตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์

วิทวัส สุขชีพ[1*] จรัญ แสนราช[2]
คณะครุศาสตร์อุตสาหกรรม มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ[1*2]
s6402042910045@email.kmutnb.ac.th[1*]

วันที่รับบทความ 13 ธันวาคม 2566
วันแก้ไขบทความ 28 พฤษภาคม 2566
วันตอบรับบทความ 29 พฤษภาคม 2566

บทคัดย่อ

การวิจัยนี้ได้ศึกษาพฤติกรรมการใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์โดยมีวัตถุประสงค์เพื่อ 1) ศึกษาประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์ 2) เพื่อศึกษาความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์ และ 3) เพื่อเปรียบเทียบระดับความตระหนักรู้ด้านภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์ โดยเป็นการวิจัยเชิงปริมาณ ด้วยการวิจัยเชิงสำรวจ ใช้แบบสอบถามเป็นเครื่องมือในการวิจัย ประชากร ได้แก่ นักเรียน นักศึกษา ศิษย์เก่า ครู อาจารย์ เจ้าหน้าที่ และผู้บริหารสถานศึกษา โดยมีขนาดตัวอย่าง 400 คน และใช้การสุ่มตัวอยางแบบชั้นภูมิและสุ่มอย่างง่ายเพื่อให้ได้จำนวนกลุ่มตัวอยางตามสัดส่วนของขนาดกลุ่มประชากร

ผลการวิจัยพบว่า ผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์ มีประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมทางไซเบอร์อยู่ในระดับน้อย (ร้อยละ 79.00) และมีความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมทางไซเบอร์อยู่ในระดับน้อย (ร้อยละ 91.75) และมีความตระหนักรู้เกี่ยวกับภัยคุกคามและอาชญากรรมทางไซเบอร์ในระดับมากที่สุด ($\bar{x}$ =4.55, SD.=0.68) เมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่า อายุ และประสบการณ์ทำงานที่ต่างกันจะมีระดับความตระหนักรู้ด้านถึงภัยคุกคามและอาชญากรรมไซเบอร์ที่แตกต่างกัน และผู้ใช้งานที่มีประสบการณ์และมีความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ในระดับมากจะมีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ในระดับมากเช่นกัน โดยผลการวิจัยนี้สามารถนำไปใช้ในออกแบบการเรียนรู้ที่เหมาะสมเพื่อป้องกันภัยคุกคามและอาชญากรรมไซเบอร์ที่สอดคล้องเหมาะสมกับปัจจุบัน ตามรูปแบบการใช้อินเทอร์เน็ตที่เปลี่ยนแปลงไปอย่างรวดเร็วเพื่อให้ผู้ใช้งานอินเทอร์เน็ตในสถานศึกษารู้เท่าทันและป้องกันตนเองได้ก่อนที่จะเกิดความไม่ปลอดภัยกับชีวิตและทรัพย์สินจากภัยและอาชญากรรมไซเบอร์ต่อไป

คำสำคัญ : การตระหนักรู้ ภัยคุกคามและอาชญากรรมไซเบอร์ ความมั่นคงปลอดภัยทางไซเบอร์ สถานศึกษา

Awareness of Cybercrime Threats and Cybercrimes by Internet Users in Educational Institutions Surin Province

Vitthawat Suksheep[1*], Charun Sanrach[2]
Department of Computer Education, Faculty of Technical Education
King Mongkut's University of Technology North Bangkok [1*,2]
s6402042910045@email.kmutnb.ac.th[1*]

Received 13 December 2022
Revised 28 May 2023
Accepted 29 May 2023

Abstract

This research studied Internet network usage behaviour in educational institutions. Surin Province. The objectives of this research were to 1) study the experience of cyber threats and cybercrime among internet network users in educational institutions, 2) to study the knowledge of cyber threats and cybercrime among internet network users in educational institutions. and 3) to compare the level of threat and cybercrime awareness among internet users in educational institutions in Surin Province. This was quantitative research that using process with exploratory research. There were questionnaires which used as a research tool. The populations are students including alumni Teachers, staff, and school administrators. The sample size was 400 people which used stratified sampling and random sampling and obtained a proportional number of cohorts of population size.

The results showed that the internet network users were found in educational institutions in Surin Province and had experience with threats and cybercrime is less level (79.00 percent). There were the greatest level of awareness of threats and cybercrime (91.75 percent). Moreover, there were the greatest level of awareness of threats and cybercrime ($\bar{x}$=4.55, SD.=0.68). When classified according to personal factors, found that the different ages and work experiences had different levels of awareness of threats and cybercrimes. Moreover, it found that the users who had experience and knowledgeable about threats and cybercrime in large level were also had aware of threats and cybercrime. The results can be used to design appropriate learning to prevent threats and cybercrime that are appropriate for today. According to the rapidly changing Internet usage patterns, so that Internet users in educational institutions can be aware and protect themselves before life and property are insecure from further threats and cybercrime.

Keywords: Awareness, Threats and Cybercrime, Cybersecurity, Educational Institutions

1. บทนำ

ภัยคุกคามและอาชญากรรมคอมพิวเตอร์เป็นสถานการณ์ที่ทวีความรุนแรงและมีการกระทำความผิดที่สลับซับซ้อนมากยิ่งขึ้นตามยุคสมัย ส่งผลให้เกิดปัญหาทางสังคมและเศรษฐกิจอย่างมากมาย โดยอาชญากรรมทางคอมพิวเตอร์ที่พบเห็นมากมาย และจากรายงานอาชญากรรมด้านความปลอดภัยบนอินเทอร์เน็ต (Internet Security Threat Report-ISTR) ฉบับที่ 22 ของไซแมนเทค ปรากฏว่ามีการตรวจพบภัยคุกคามใหม่ ๆ เพิ่มขึ้นบนอุปกรณ์พกพา และแนวโน้มดังกล่าวยังคงเพิ่มขึ้นอย่างต่อเนื่อง เช่น การละเมิดทรัพย์สินทางปัญญา การลักลอบเข้าถึง แก้ไข เปลี่ยนแปลงการทำลายระบบข้อมูลสำคัญ การขโมยข้อมูลระบุตัวตน การปลอมหรือสวมรอย เป็นต้น (ชฎาภรณ์ สิงห์แก้ว. 2564 : 541) นอกจากนี้ ประเทศไทยได้ถูกจัดเป็นประเทศที่มีการป้องกันภัยคุกคามไซเบอร์ต่ำกว่ามาตรฐาน และติดอันดับ 15 ของโลกในเรื่องประเทศที่มีความเสี่ยงด้านไซเบอร์ (Marketing Oops!. 2018) ขณะที่ประเทศไทยมีการพัฒนาด้านธุรกรรมทางอิเล็กทรอนิกส์มากเท่าใด ภัยคุกคามในโลกไซเบอร์ถือได้ว่าเป็นภัยร้ายที่ประชาชนคนไทยต้องเผชิญหน้าอย่างหลีกเลี่ยงไม่ได้ อาทิเช่น การปลอมบัญชีโซเชียลมีเดีย การขโมยข้อมูล การโจมตีระบบ และภัยคุกคามไซเบอร์อื่น ๆ ซึ่งปัจจุบันภัยคุกคามทางไซเบอร์ในประเทศไทยมีจำนวนที่เพิ่มสูงขึ้นและทวีความรุนแรงขึ้นเรื่อย ๆ ความสามารถในการเข้าถึงโครงข่ายไซเบอร์ของประชากรในประเทศไทยได้เพิ่มขึ้นอย่างก้าวกระโดด จึงทำให้ความเสี่ยงด้านอาชญากรรมไซเบอร์มีสูงขึ้นหลายเท่าตัวและเป็นภัยคุกคามที่จะถูกยกระดับในเชิงยุทธศาสตร์ของประเทศ และการที่สิ่งต่าง ๆ ถูกเชื่อมโยงทุกสิ่งทุกอย่างเข้าสู่โลกอินเทอร์เน็ตทำให้ปัจจุบันมีการสั่งการควบคุมใช้งานอุปกรณ์ต่าง ๆ ผ่านทางเครือข่ายอินเทอร์เน็ตได้อย่างง่ายดาย จึงทำให้ความสามารถของอาชญากรทางไซเบอร์ที่มี จำนวนเพิ่มมากขึ้น ส่งผลกระทบโดยตรงต่อความปลอดภัยระบบสารสนเทศขององค์กร ทำให้การดำเนินงานขององค์กรต้องถูกชะงัก สร้างความเสียหาย ทำลายความน่าเชื่อถือขององค์กร (เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี. 2565 : 4)

สถาบันการศึกษาใช้อินเทอร์เน็ตเพื่ออำนวยความสะดวกในการสืบค้นข้อมูลและถือได้ว่าเป็นสิ่งสำคัญในการเรียนรู้ จากข้อมูลดังกล่าวชี้ให้เห็นว่าผู้ใช้งานอินเทอร์เน็ตต้องให้ความสำคัญและมีองค์ความรู้ที่ส่งผลต่อความมั่นคงและปลอดภัยทางไซเบอร์ของสถานศึกษา ในปัจจุบันในสถานศึกษามีการลงทุนจัดซื้ออุปกรณ์เพื่อสร้างระบบรักษาความปลอดภัยทางไซเบอร์มากมาย แต่อาจมีความเสี่ยงได้หากผู้ใช้งานไม่เกิดการเรียนรู้ในการป้องกันตนเองให้ห่างไกลจากภัยคุกคามและอาชญากรรมทางไซเบอร์ได้ ดังนั้นการศึกษาถึงความตระหนักรู้ถึงภัยคุกคามและอาชญากรรมทางไซเบอร์ของผู้ใช้งานอินเทอร์เน็ตในสถานศึกษาจะสะท้อนการพัฒนาแนวทางในการกำหนดนโยบายด้านความมั่นคงปลอดภัยทางไซเบอร์ อันจะนำไปสู่การออกแบบกระบวนการสร้างองค์ความรู้เพื่อสร้างความตระหนักรู้ด้านภัยคุกคามและอาชญากรรมทางไซเบอร์ต่อไป

2. วัตถุประสงค์

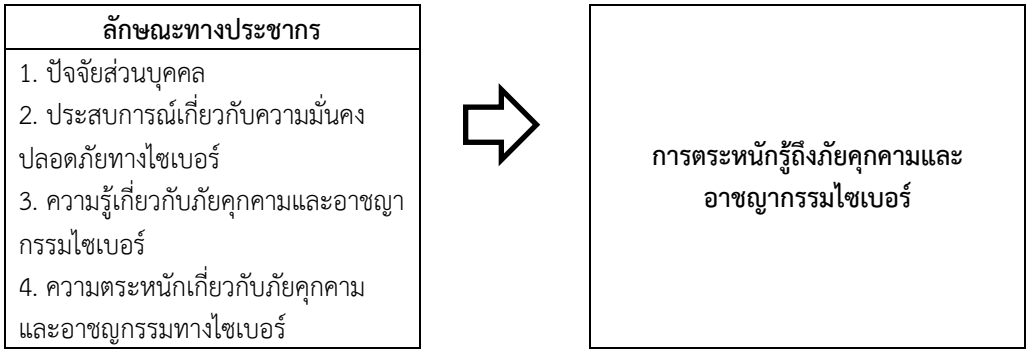
2.1 เพื่อศึกษาประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์

2.2 เพื่อศึกษาความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์

2.3 เพื่อเปรียบเทียบระดับความตระหนักรู้ด้านภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์

3. วิธีการวิจัย

งานวิจัยนี้ใช้วิธีวิจัยเชิงปริมาณ เพื่อศึกษาถึงความตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์ โดยดำเนินการตามขั้นตอน ดังนี้



รูปที่ 1 กรอบแนวคิดในการวิจัย

3.1 ประชากรและกลุ่มตัวอย่าง ได้แก่ผู้ใช้อินเทอร์เน็ตในสถานศึกษาที่มีอายุตั้งแต่ 15 ปี ขึ้นไป ในสถานศึกษาจังหวัดสุรินทร์ จำนวน 400 คน โดยใช้สูตรการหาขนาดกลุ่มตัวอย่างของ Cochran (1977) กรณีที่ไม่ทราบขนาดประชากร โดยใช้สูตรดังนี้

$$n = \frac{1(1-P)(Z)^2}{e^2}$$

เมื่อ n แทน ขนาดตัวอย่าง
P แทน สัดส่วนของประชากรที่ผู้วิจัยกำลังสุ่ม (ในที่นี้กำหนดไวที่ 0.50)
Z แทน ค่าสถิติ Z ที่ระดับความเชื่อมั่นร้อยละ 95 (มีคาเทากับ 1.96)
e แทน คาความคลาดเคลื่อนจากการสุ่มตัวอย่างที่ยอมใหเกิดขึ้นได้ (ในที่นี้กำหนดไวที่รอยละ 5 หรือ 0.05)

แทนคาในสูตร

$$n = \frac{(0.50)(1-0.50)(1.96)^2}{(0.05)^2}$$

$$= 384.16$$

จากการคำนวณจะได้ขนาดตัวอย่าง 384 คน แต่เพื่อป้องกันความผิดพลาดงานวิจัยครั้งนี้จะใช้ขนาดตัวอย่าง 400 คน

3.2 การสร้างเครื่องมือที่ใช้ในการวิจัย เครื่องมือที่ใช้ในการวิจัยได้แก่แบบสอบถามแบบ และทำการทดสอบคุณภาพเครื่องมือในการวิจัย โดยทำการทดสอบความเที่ยงตรงของเนื้อหา โดยการหาค่าดัชนีความสอดคล้อง (IOC : Index of Item – Objective Congruence) โดยเลือกข้อคำถามที่มีค่า IOC มากกว่า 0.5 จากผู้เชี่ยวชาญ จำนวน 3 ท่าน และความน่าเชื่อถือโดยนำแบบสอบถามไปทดลองใช้จำนวน 30 ชุด ผู้วิจัยได้กำหนดลักษณะของเครื่องมือในการวิจัยดังนี้

ตอนที่ 1 ลักษณะทางประชากร เกี่ยวกับปัจจัยส่วนบุคคล จำนวน 5 ข้อ ได้แก่ เพศ อายุ สถานภาพ ประสบการณ์ ทำงาน และระดับการศึกษา

ตอนที่ 2 ประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ซึ่งสามารถตอบได้มากกว่าหนึ่งคำตอบ จำนวน 10 ข้อ โดยกำหนดเกณฑ์การให้คะแนน คือ มีประสบการณ์ = 1 และ ไม่มีประสบการณ์ = 0 แล้วนำมารวมคะแนนเพื่อนำไปใช้ในการตอบสมมติฐานและแบ่งตามระดับประสบการณ์เป็น 3 ระดับ ได้แก่ 1) 0 – 3 คะแนน คือ มีประสบการณ์น้อย 2) 4 – 6 คะแนน คือ มีประสบการณ์ปานกลาง และ 3) 7-10 คะแนน คือ มีประสบการณ์มาก

ตอนที่ 3 ความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ จำนวน 13 ข้อ ให้ตอบเพียง 2 ตัวเลือกเท่านั้นคือ “ใช่” และ “ไม่ใช่” โดยข้อความที่ถูกต้องจะได้ 1 คะแนน แล้วนำคะแนนที่ได้มารวมเพื่อใช้ในการทดสอบสมมติฐาน และแบ่งตามระดับความรู้เป็น 3 ระดับ ได้แก่ 1) 0 – 4 คะแนน คือ มีความรู้น้อย 2) 5 – 9 คะแนน คือ มีความรู้ปานกลาง และ 3) 10-13 คะแนน คือ มีความรู้มาก

ตอนที่ 4 ความตระหนักเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ประกอบด้วยข้อคำถามแบบมาตราส่วนประมาณค่า (Rating Scale) ซึ่งมีเกณฑ์ในการกำหนดค่าน้ำหนักของการประเมิน 5 ระดับ ตามวิธีของลิเคิร์ท (Likert) (ธานินทร์ ศิลป์จารุ, 2557: 77) จำนวน 5 ด้าน ได้แก่ 1) ด้านความปลอดภัยของระบบสารสนเทศ 2) ด้านการกลั่นแกล้งกันบนโลกไซเบอร์ 3) ด้านการสร้างความเสียหาย 4) ด้านการสร้างความเดือดร้อนรำคาญ และ 5) ด้านกลุ่มอาชญากรหรือมิจฉาชีพ รวมทั้งสิ้น 22 ข้อ โดยระบุเกณฑ์การแปลผล ดังนี้ ตระหนักมากที่สุด คือ 5 ตระหนักมาก คือ 4 ตระหนักปานกลาง คือ 3 ตระหนักน้อย คือ 2 และตระหนักน้อยที่สุด คือ 1 และนำมาหาค่าเฉลี่ยโดยแบ่งระดับความตระหนักเกี่ยวกับภัยคุกคามและอาชญากรรมทางไซเบอร์

ตอนที่ 5 เป็นแบบสอบถามเพื่อรับฟังข้อเสนอแนะเพิ่มเติม

3.3 คุณภาพของเครื่องมือวัด ผู้วิจัยได้ทดสอบความเที่ยงตรง ความเชื่อมั่นและค่าอำนาจจำแนกเป็นรายข้อ โดยทำการตรวจสอบความเที่ยงตรงเชิงเนื้อหาผ่านการพิจารณาของผู้เชี่ยวชาญและหาค่าความเชื่อมั่น (Reliability) โดยใช้วิธีหาค่าสัมประสิทธิ์แอลฟา (Alpha Coefficient) ตามวิธีของ Cronbach ซึ่งด้านประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ได้ค่าสัมประสิทธิ์แอลฟาระหว่าง 0.863 - 0.882 ด้านความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ได้ค่าสัมประสิทธิ์แอลฟาระหว่าง 0.893- 0.919 และด้านความตระหนักเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ อยู่ระหว่าง 0.941 - 0.949 การวิเคราะห์หาค่าอำนาจจำแนกเป็นรายข้อ (Discriminant Power) ของแต่ละด้านโดยใช้เทคนิค Corrected Item – total Correlation ซึ่งด้านประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ได้ค่าอำนาจจำแนก (r) ระหว่าง 0.491-0.753 ด้านความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ได้ค่าอำนาจจำแนก (r) ระหว่าง 0.415 – 0.835 และด้านความตระหนักเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ได้ค่าอำนาจจำแนก (r) ระหว่าง 0.442 – 0.890 สอดคล้องกับ Nunnally (Nunnally, J. C. 1978) ได้กล่าวว่าการทดสอบค่าอำนาจจำแนกเกินกว่า 0.20 เป็นค่าที่ยอมรับได้

3.4 การเก็บและรวบรวมข้อมูล โดยผู้วิจัยได้ประสานสถาบันการศึกษา แล้วนำแบบสอบถามที่จัดทำขึ้นไปมอบให้ผู้ประสานงานในแต่ละสถาบันการศึกษา และแบบสอบถามออนไลน์เพื่อให้ผู้ที่มีความประสงค์ตอบคำถามและได้ชี้แจงวัตถุประสงค์ของการวิจัยเป็นลายลักษณ์อักษรไว้อย่างชัดเจน โดยเริ่มเก็บข้อมูลตั้งแต่เดือนมกราคม - พฤษภาคม 2565

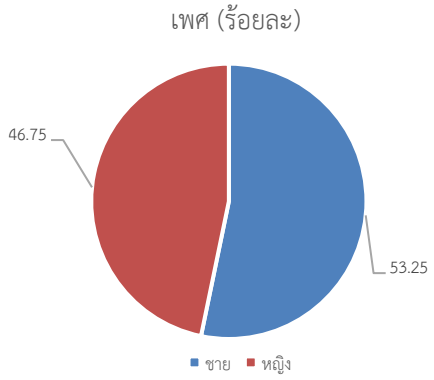
3.5 การวิเคราะห์ข้อมูล ผู้วิจัยได้นำข้อมูลที่ได้มาวิเคราะห์ประมวลผลทางสถิติ และสามารถแบ่งการวิเคราะห์ข้อมูลได้ 2 ประเภท

3.5.1 สถิติเชิงพรรณนา (Descriptive Statistics) ได้แก่การแจกแจงความถี่ (Frequency) แบบค่าร้อยละ (Percentage) ค่าเฉลี่ย (Mean) และส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่อแสดงรายละเอียดของข้อมูลและอธิบายค่าของข้อมูล

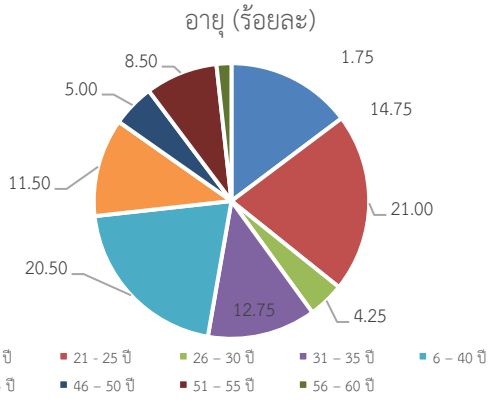
3.5.2 สถิติเชิงอนุมาณ (Inferential Statistics) การนำข้อมูลที่ได้มาจากกลุ่มตัวอย่าง มาทดสอบหาความสัมพันธ์ระหว่างตัวแปรอิสระ (Independent Variables) กับตัวแปรตาม(Dependent Variables) โดยใช้สถิติ One way ANOVA ทดสอบความแตกต่างจะทำการทดสอบด้วยการเปรียบเทียบเป็นรายคู่ด้วยวิธี LSDและ Pearson Correlation ในการทดสอบสมมติฐาน

4. ผลการวิจัย

4.1 ผลการวิเคราะห์ข้อมูลทางประชากร พบว่า ส่วนใหญ่เป็นเพศชาย จำนวน 213 คน คิดเป็นร้อยละ 53.25 และเป็นเพศหญิง จำนวน 187 คน คิดเป็นร้อยละ 46.75 ดังรูปที่ 2 และมีอายุระหว่าง 21-25 ปี จำนวน 84 คน คิดเป็นร้อยละ 21.00 รองลงมาคือ 36-40 ปี จำนวน 82 คน คิดเป็นร้อยละ 20.50 และน้อยที่สุดคือ 56-60 ปี จำนวน 7 คน คิดเป็นร้อยละ 1.75 ดังรูปที่ 3

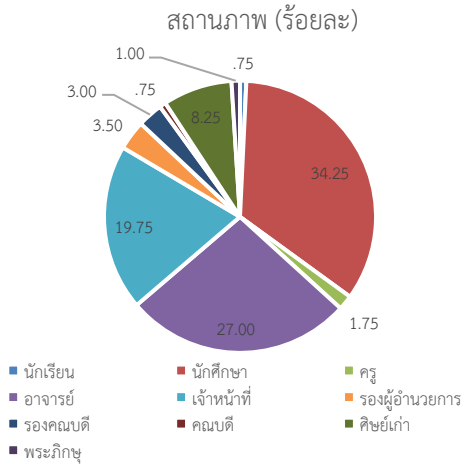


รูปที่ 1 เพศ

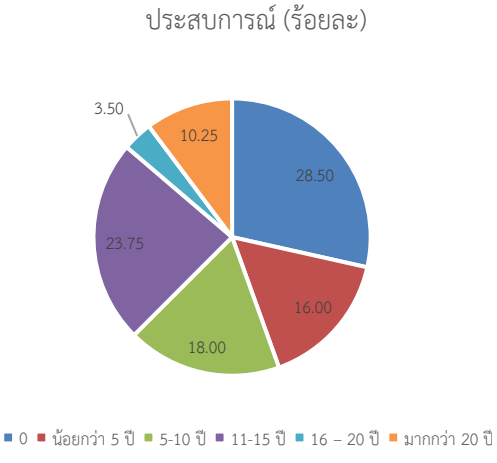


รูปที่ 2 อายุ

นอกจากนี้ยังพบว่า มีสถานภาพเป็นนักศึกษามากที่สุด จำนวน 137 คน คิดเป็นร้อยละ 34.25 รองลงมา คือ เป็นอาจารย์ จำนวน 108 คน คิดเป็นร้อยล 27.00 และน้อยที่สุดคือเป็นนักเรียน จำนวน 3 คน คิดเป็นร้อยละ 0.75 ดังรูปที่ 4

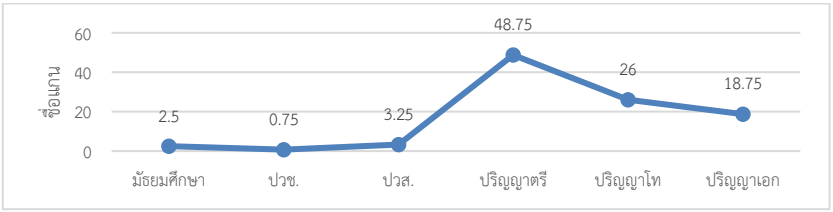


รูปที่ 4 สถานภาพ



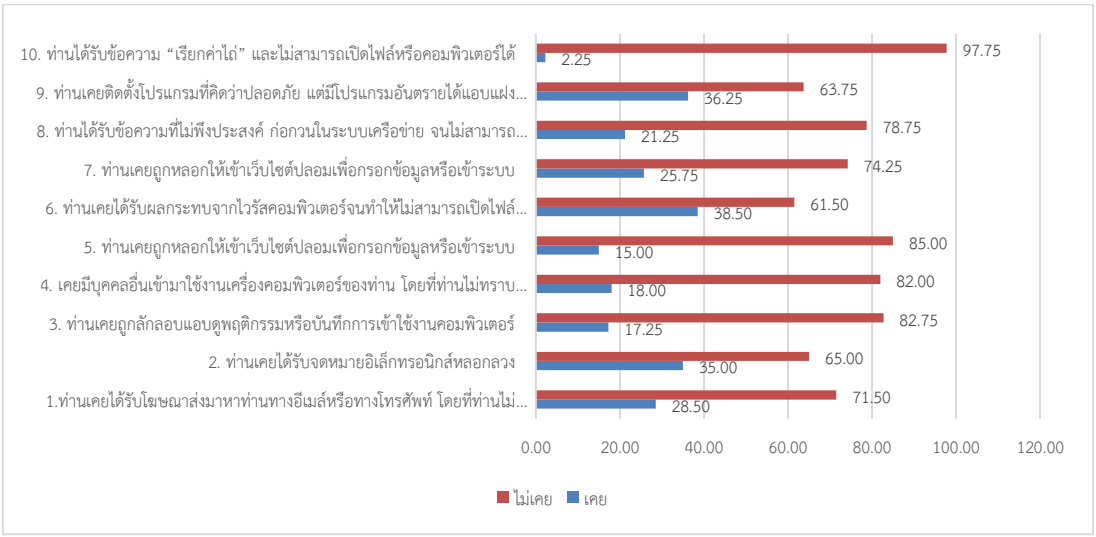
รูปที่ 5 ประสบการณ์

ในด้านประสบการณ์ของผู้ตอบแบบสอบถามส่วนใหญ่ คือไม่มีประสบการณ์ จำนวน 114 คน คิดเป็นร้อยละ 28.50 รองลงมาอยู่ระหว่าง 11-15 ปี จำนวน 95 คน คิดเป็นร้อยละ 23.75 และน้อยที่สุดอยู่ระหว่าง 16-20 ปี จำนวน 14 คน คิดเป็นร้อยละ 3.50 ดังรูปที่ 5 และระดับการศึกษาของผู้ตอบแบบสอบถาม คือปริญญาตรี จำนวน 195 คน คิดเป็นร้อยละ 48.75 รองลงมาคือปริญญาโท จำนวน 104 คน คิดเป็นร้อยละ 26.00 และน้อยที่สุดคือ ประกาศนียบัตรวิชาชีพ (ปวช.) จำนวน 3 คน คิดเป็นร้อยละ 0.75 ดังรูปที่ 6



รูปที่ 6 ระดับการศึกษา

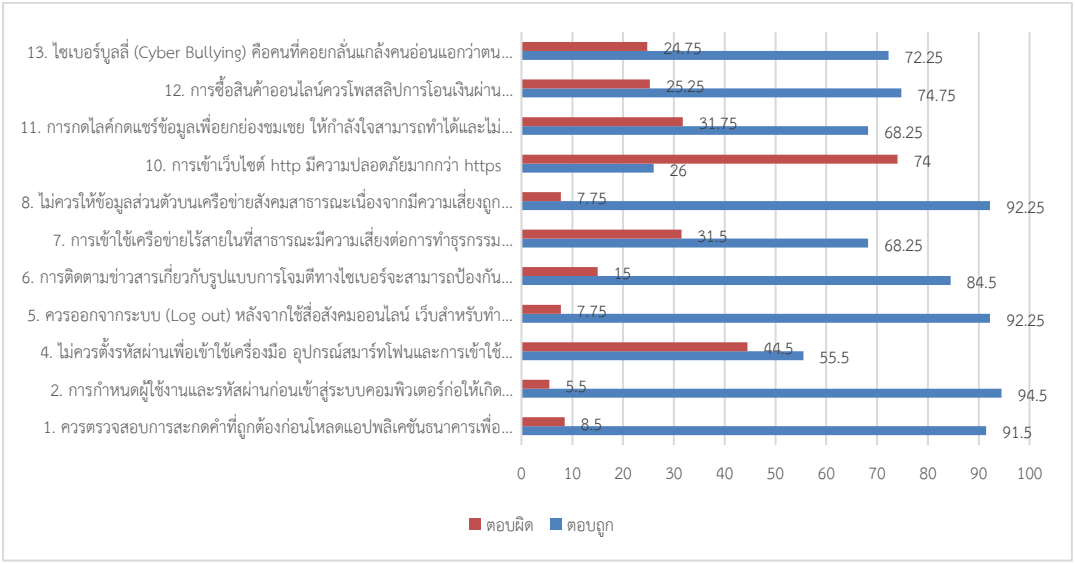
4.2 ประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ พบว่า ส่วนใหญ่เคยได้รับข้อความที่ไม่พึงประสงค์ก่อกวนในระบบเครือข่าย จนไม่สามารถทำงานได้ มากที่สุด จำนวน 154 คน คิดเป็นร้อยละ 38.50 และไม่เคย จำนวน 246 คน คิดเป็นร้อยละ 61.50 รองลงมา ท่านเคยติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายได้แอบแฝงมาด้วย จำนวน 145 คน คิดเป็นร้อยละ 36.25 และไม่เคย จำนวน 255 คน คิดเป็นร้อยละ 63.75 และน้อยที่สุดคือ เคยได้รับข้อความ “เรียกค่าไถ่” และไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จำนวน 9 คน คิดเป็นร้อยละ 2.25 และ ไม่เคย จำนวน 391 คน คิดเป็นร้อยละ 97.75 ดังรูปที่ 7 และสามารถจัดกลุ่มระดับประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ได้ 3 ระดับ โดยพบว่า ส่วนใหญ่มีประสบการณ์น้อย จำนวน 316 คน คิดเป็นร้อยละ 79.00 รองลงมามีประสบการณ์ปานกลาง จำนวน 46 คน คิดเป็นร้อยละ 12.25 และ มีประสบการณ์มาก จำนวน 35 คน คิดเป็นร้อยละ 8.75



รูปที่ 7 ประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์

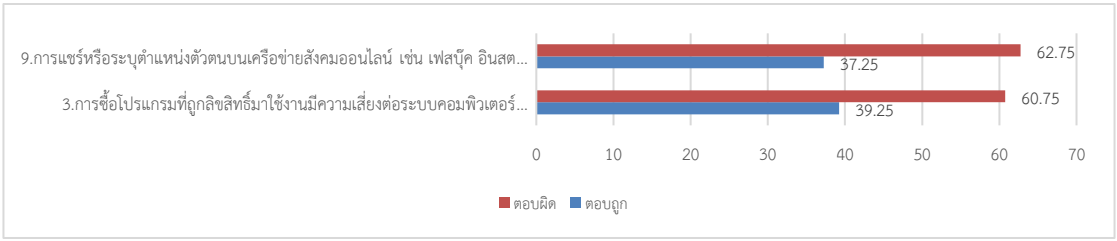
4.3 ความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ พบว่าข้อที่ตอบถูกคือข้อที่ “ใช่” ได้แก่ข้อ 1 2 4 5 6 7 8 10 11 12 และ 13 ที่ตอบถูกมากที่สุดคือ การกำหนดผู้ใช้งานและรหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ก่อให้เกิดความปลอดภัยในการเข้าใช้งาน จำนวน 378 คน คิดเป็นร้อยละ 94.50 และตอบผิด จำนวน 22 คน คิดเป็นร้อยละ 4.80 รองลงมาคือ ไม่ควรให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะเนื่องจากมีความเสี่ยงถูกลักลอบ

ข้อมูล จำนวน 369 คน คิดเป็นร้อยละ 92.25 และตอบผิด จำนวน 21 คน คิดเป็นร้อยละ 7.75 และน้อยที่สุดคือ การเข้าเว็บไซต์ http มีความปลอดภัยมากกว่า https จำนวน 104 คน คิดเป็นร้อยละ 26 ดังรูปที่ 8



รูปที่ 8 ร้อยละของผู้ตอบถูก

ข้อที่ตอบถูกคือข้อที่ “ไม่ใช่” ได้แก่ข้อ 3 และ 9 ที่ตอบถูกมากที่สุดคือ การซื้อโปรแกรมที่ถูกลิขสิทธิ์มาใช้งานมีความเสี่ยงต่อระบบคอมพิวเตอร์คล้ายคลึงกับโปรแกรมที่แชร์ให้โหลดได้ฟรีในอินเทอร์เน็ต จำนวน 157 คน คิดเป็นร้อยละ 39.25 และตอบผิด จำนวน 243 คน คิดเป็นร้อยละ 60.75 รองลงมา คือการแชร์หรือระบุตำแหน่งตัวตนบนเครือข่ายสังคมออนไลน์ เช่น เฟสบุ๊ค อินสตราแกรม สามารถทำได้และไม่ได้รับอันตรายใด ๆ จำนวน 149 คน คิดเป็นร้อยละ 37.25 และตอบผิด จำนวน 251 คน คิดเป็นร้อยละ 62.75 ดังรูปที่ 9



รูปที่ 9 ร้อยละของผู้ตอบผิด

โดยสามารถจัดกลุ่มความรู้ได้ 3 ระดับ โดยพบว่ามีความรู้มาก จำนวน 367 คน คิดเป็นร้อยละ 91.75 รองลงมา คือ มีความรู้มาก จำนวน 21 คน คิดเป็นร้อยละ 5.25 และ น้อยที่สุด คือ มีความรู้น้อย จำนวน 12 คน คิดเป็นร้อยละ 3

4.4 ความตระหนักเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ มีรายละเอียดดังตารางที่ 1

ตารางที่ 1 ความตระหนักเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์

ความตระหนักเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์	$\bar{x}$	S.D.	ระดับความตระหนัก
ด้านความปลอดภัยของระบบสารสนเทศ	4.59	0.66	มากที่สุด
ด้านการกลั่นแกล้งกันบนโลกไซเบอร์	4.02	0.96	มาก
ด้านสร้างความเสียหาย	4.66	0.58	มากที่สุด
ด้านสร้างความเดือดร้อนรำคาญ	4.79	0.49	มากที่สุด
ด้านกลุ่มอาชญากรหรือมิจฉาชีพ	4.68	0.59	มากที่สุด
ค่าเฉลี่ยรวมทุกด้าน	**4.55**	**0.68**	**มากที่สุด**

ตารางที่ 1 ความตระหนักเกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์มีค่าเฉลี่ยรวมทุกด้าน อยู่ในระดับความตระหนัก ในระดับมากที่สุด ($\bar{x}$ = 4.55, S.D.= 0.68) เมื่อพิจารณาเป็นรายด้านพบว่า ด้านสร้างความเดือดร้อนรำคาญ อยู่ในระดับความตระหนักมากที่สุด ($\bar{x}$ = 4.79, S.D.= 0.49) รองลงมาคือ ด้านกลุ่มอาชญากรหรือมิจฉาชีพ อยู่ในระดับความตระหนักมากที่สุด ($\bar{x}$ = 4.68, S.D.= 0.59) และระดับความตระหนักน้อยที่สุด คือ ด้านการกลั่นแกล้งกันบนโลกไซเบอร์ อยู่ในระดับมาก ($\bar{x}$ = 4.02, S.D.= 0.96)

4.5 การทดสอบสมมติฐาน

4.5.1 ลักษณะทางประชากรมีผลต่อความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้อินเทอร์เน็ตในสถานศึกษาจำแนกตามอายุ

4.5.1.2 อายุมีผลต่อความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้อินเทอร์เน็ตในสถานศึกษา

ตารางที่ 2 การวิเคราะห์ความแปรปรวนทางเดียวของความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้อินเทอร์เน็ต จำแนกตามอายุ

แหล่งที่มา	SS	df	MS	F	p
ระหว่างกลุ่ม	3.612	8	.451	3.229*	.001
ภายในกลุ่ม	54.662	391	.140		
รวม	58.274	399			

* มีนัยสำคัญทางสถิติที่ระดับ .05

ตารางที่ 2 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ อายุที่ต่างกันมีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 กล่าวคือ อายุมีความสัมพันธ์กับความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ จึงทำการทดสอบความแตกต่างของค่าเฉลี่ยเป็นรายคู่ด้วยวิธีการ LSD ดังตารางที่ 3

ตารางที่ 3 ผลการทดสอบความแตกต่างของค่าเฉลี่ยเป็นรายคู่ของอายุ ด้วยวิธีการ LSD

อายุ	$\bar{x}$	15-20 ปี	21-25ปี	26–30ปี	31–35ปี	36–40ปี	41–45ปี	46–50ปี	51–55ปี	56–60ปี
		4.57	4.58	4.71	4.60	4.70	4.56	4.36	4.45	4.31
15 - 20 ปี	4.57	-	-0.10	-.141	-.033	-.132*	.009	.206*	.124	.258
21 - 25 ปี	4.58		-	-.131	-.023	-.122*	.019	.216*	.134	.268
26 – 30 ปี	4.71				.108	.009	.150	.348*	.265*	.400*
31 – 35 ปี	4.60					-.099	.042	.240*	.157	.292
36 – 40 ปี	4.70						.141*	.339*	.256*	.391*
41 – 45 ปี	4.56							.198*	.115	.250
46 – 50 ปี	4.36								-.083	.052
51 – 55 ปี	4.45									.135
56 – 60 ปี	4.31									-

*มีนัยสำคัญทางสถิติที่ระดับ .05

ตารางที่ 3 เมื่อเปรียบเทียบรายคู่ที่ 1 พบว่า พบว่า ผู้ที่มีอายุ 36 - 40 ปี มีค่าเฉลี่ยความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์มากกว่า ผู้มีอายุ 15 - 20 ปี กับและอายุ 46 - 50 ปี เมื่อเปรียบเทียบรายคู่ที่ 2 พบว่า ผู้มีอายุ 36 - 40 ปี มีค่าเฉลี่ยความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์มากกว่า ผู้ที่มีอายุ 21 - 25 ปี กับและอายุ 46 - 50 ปี เมื่อเปรียบเทียบรายคู่ที่ 3 พบว่า ผู้มีอายุ 26 – 30 ปี มีค่าเฉลี่ยความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์มากกว่า ผู้มีอายุ 46 - 50 ปี เมื่อเปรียบเทียบรายคู่ที่ 4 พบว่า ผู้ที่มีอายุ 31 – 35 ปี มีค่าเฉลี่ยความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์มากกว่า ผู้ที่มีอายุ 46 - 50 ปี เมื่อเปรียบเทียบรายคู่ที่ 5 พบว่า ผู้ที่มีอายุ 36 – 40 ปี มีค่าเฉลี่ยความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์มากกว่า ผู้มีอายุ 46 - 50 ปี อายุ 51-55 ปี และ อายุ 56-60 ปี และดเมื่อเปรียบเทียบรายคู่ที่ 6 พบว่า และผู้ที่มีอายุ 41 – 45 ปี มีค่าเฉลี่ยความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์มากว่าผู้มีอายุ 46 - 50 ปี อย่างมีนัยสำคัญทางสถิติที่ระดับ .05

4.5.2 ลักษณะทางประชากรมีผลต่อความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้อินเทอร์เน็ตในสถานศึกษาจำแนกตามประสบการณ์ทำงาน

ตารางที่ 4 การวิเคราะห์ความแปรปรวนทางเดียวของความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้อินเทอร์เน็ต จำแนกตามประสบการณ์ทำงาน

แหล่งที่มา	SS	df	MS	F	p
ระหว่างกลุ่ม	3.810	5	.762	5.513*	.000
ภายในกลุ่ม	54.463	394	.138		
รวม	58.274	399			

*มีนัยสำคัญทางสถิติที่ระดับ .05

ตารางที่ 4 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ ประสบการณ์ทำงานที่ต่างกันมีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05 กล่าวคือ ประสบการณ์มีความสัมพันธ์

กับความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ จึงทำการทดสอบความแตกต่างของค่าเฉลี่ยเป็นรายคู่ด้วยวิธีการ LSD ดังตารางที่ 5

ตารางที่ 5 ผลการทดสอบความแตกต่างของค่าเฉลี่ยเป็นรายคู่ของประสบการณ์ทำงาน ด้วยวิธีการ LSD

ประสบการณ์	$\bar{x}$	0	< 5 ปี	5-10 ปี	11-15 ปี	16-20 ปี	> 20 ปี
		4.53	4.65	4.59	4.69	4.21	4.51
0	4.53	-	-.118*	-.060	-.159*	.321*	.017
< 5 ปี	4.65			.057	-.041	.439*	.134
5-10 ปี	4.59				-.099	.381*	.077
11-15 ปี	4.69					.480*	.175*
16-20 ปี	4.21						-.304*
> 20 ปี	4.51						-

*มีนัยสำคัญทางสถิติที่ระดับ .05

ตารางที่ 5 พบว่า ผู้ไม่มีประสบการณ์ กับผู้มีประสบการณ์น้อยกว่า 5 ปี กับประสบการณ์ 11-15 ปี และประสบการณ์ 16-20 ปี มีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์มากกว่า ผู้มีประสบการณ์น้อยกว่า 5 ปี กับประสบการณ์ 16-20 ปี มีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์แตกต่างกัน ผู้มีประสบการณ์ 5-10 ปี กับประสบการณ์ 16-20 ปี มีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์แตกต่างกัน ผู้มีประสบการณ์ 11-15 ปี กับผู้มีประสบการณ์ 16-20 ปี กับมากกว่า 20 ปี มีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์แตกต่างกัน และผู้มีประสบการณ์ 16-20 ปี กับมากกว่า 20 ปี มีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์แตกต่างกันอย่างมีนัยสำคัญทางสถิติที่ระดับ .05

4.5.3 ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานอินเทอร์เน็ตในสถานศึกษา

ตารางที่ 6 ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์

ตัวแปร	ความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์	
	r	p
ประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์	.952*	.003

*มีนัยสำคัญทางสถิติที่ระดับ .05

ตารางที่ 6 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ ประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรม ไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้อินเทอร์เน็ตในสถานศึกษาที่ระดับนัยสำคัญ .05 ($p < .05$) โดยมีผลบวกคือ ผู้ใช้งานมีประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์มาก จะมีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์มากเช่นกัน

ตารางที่ 7 ค่าสัมประสิทธิ์สหสัมพันธ์ระหว่างความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์

ตัวแปร	ความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์	
	r	p
ความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์	-.332**	.000

** มีนัยสำคัญทางสถิติที่ระดับ 0.01

ตารางที่ 7 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ ความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ มีผลต่อความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้อินเทอร์เน็ตในสถานศึกษาที่ระดับนัยสำคัญ .01 ($p < .01$) โดยมีผลลบคือ ผู้ใช้งานมีความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์มาก จะมีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์น้อยด้วย

5. อภิปรายผลและสรุปผล

จากผลการวิจัยเรื่องการตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์ พบว่า กลุ่มตัวอย่างมีความตระหนักรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ในภาพรวมอยู่ในระดับมาก โดยผู้วิจัยเห็นว่ามีผลสืบเนื่องจากปัจจุบันมีการนำเสนอข้อมูลผ่านสื่อโซเชียลมีเดียอย่างแพร่หลาย สอดคล้องกับเมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี (2565 : 1-2) ที่ได้ศึกษาเกี่ยวกับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร ที่กลุ่มตัวอย่างมีความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับมาก เนื่องจากสถาบันการศึกษามีการจัดหลักสูตร รายวิชาเพื่อให้นักศึกษาได้เรียนรู้เกี่ยวกับจริยธรรมในการใช้คอมพิวเตอร์ นอกจากนี้ยังได้รับความรู้ข่าวสารและประ สบการณ์จากรับฟังข่าวจากสื่อโซเชียลต่าง ๆ จึงเป็นที่สนใจ จึงทำให้บุคลากรทุกระดับในสถาบันการศึกษาได้เกิดการเรียนรู้ เกิดความเข้าใจและพยายามป้องกันตนเองจากภัยคุกคามและอาชญากรรมไซเบอร์ ส่งผลให้เกิดความตระหนักรู้ตามที่กุลวดี ราชภักดี (2545 : 38) ได้กล่าวว่า ความตระหนัก คือความรู้สึก นึกคิดที่บุคคลได้รับจากประสบการณ์แล้วเกิดความเข้าใจที่ยอมรับและเกิดการแสดงพฤติกรรมตอบสนอง ซึ่งเมื่อมีอายุและประสบการณ์จากการทำงานมากจะส่งผลต่อการเรียนรู้ การสร้างคุ้นเคยเกี่ยวกับการใช้อินเทอร์เน็ต

ผลการวิจัยในลักษณะประชากรที่พบว่า ผู้ใช้งานอินเทอร์เน็ตในสถานศึกษาที่มี อายุและประสบการณ์การทำงานที่ต่างกันมีระดับความตระหนักรู้กับภัยคุกคามและอาชญากรรมไซเบอร์ที่แตกต่างกัน ในด้านประสบการณ์เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ คือ เคยได้รับข้อความที่ไม่พึงประสงค์ส่งมาในอีเมล์ หรือการได้รับการก่อกวนในระบบเครือข่าย เช่น ข้อความที่ส่งมายังอีเมล์ ข้อความส่งมาผ่านทางโซเชียลมีเดีย หรือเว็บโฆษณาก่อกวน ก่อให้เกิดความรำคาญจนไม่สามารถทำงานได้ จึงจำเป็นอย่างยิ่งที่สถาบันการศึกษาต้องมีมาตรการรักษาความมั่นคงในเครือข่ายคอมพิวเตอร์ของหน่วยงานภาครัฐ ซึ่งผู้วิจัยเห็นว่าอายุและประสบการณ์ที่ได้รับนั้นสำคัญในการตระหนักรู้กับภัยคุกคามดังกล่าวนี้ สอดคล้องกับงานวิจัยของ ชิษณุพงศ์ ธนูทอง (2557) ที่ได้ศึกษาเรื่องการพัฒนาการรักษาความมั่นคงในระบบเครือข่ายหน่วยงานภาครัฐ ที่ได้เสนอแนวทางการแก้ไขปัญหาด้านการพัฒนารักษาความมั่นคงของระบบเครือข่าย โดยการให้ความรู้ความเข้าใจ คำปรึกษาและประสานงานกับผู้ที่รับผิดชองงานด้านความมั่นคงปลอดภัย ควรมีการตรวจสอบการประเมินความเสี่ยงของระบบสารสนเทศ และจัดฝึกอบรมให้ความรู้แก่บุคลากรให้หน่วยงานภาครัฐ ในด้านความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์ ส่วนใหญ่มีความรู้เกี่ยวกับการกำหนดผู้ใช้งานและรหัสผ่านก่อนเข้าสู่ระบบคอมพิวเตอร์ก่อให้เกิดความปลอดภัยในการเข้าใช้งานมากที่สุด สอดคล้องกับสุทาเทพ รุณเรศ (2561 : 61) ที่ได้ศึกษาเกี่ยวกับปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร ที่พบว่าผู้ใช้งานอินเทอร์เน็ตมีการตั้งรหัสผ่าน โดยตั้งปนกันทั้งตัวอักษรใหญ่ -เล็ก

ตัวเลข สัญลักษณ์พิเศษ และยาวอย่างน้อย 8 ตัวอักษร เพื่อป้องกันความปลอดภัยของข้อมูล นอกจากนี้คือไม่ควรให้ข้อมูลส่วนตัวบนเครือข่ายสังคมสาธารณะเนื่องจากมีความเสี่ยงถูกลักลอบข้อมูล และควรเข้าใช้เว็บไซต์ที่มีโปรโตคอล https เนื่องจากมีความปลอดภัยมากกว่าโปรโตคอล http สอดคล้องกับ เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี (2565:1-2) ที่พบว่าบุคลากรของบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร ที่ได้รับการอบรมเสริมสร้างความตระหนักรู้ทางไซเบอร์อย่างสม่ำเสมอจะมีความตระหนักรู้เกี่ยวกับเรื่องการกำหนดรหัสผ่าน การป้องกันการถูกโจมตีทางไซเบอร์ และการหลอกลวงทางไซเบอร์ผ่านสื่อต่าง ๆ นอกจากนี้ ยังพบว่าผู้ใช้งานมีประสบการณ์และความรู้เกี่ยวกับภัยคุกคามและอาชญากรรมไซเบอร์มากจะมีความตระหนักถึงภัยคุกคามและอาชญากรรมไซเบอร์ในระดับมาก สอดคล้องกับงานวิจัยของ วาสนา อุทัยแสง (2559 : 8) ที่กล่าวว่าบุคลากรที่เคยมีประสบการณ์ตรงจะมีระดับความตระหนักรู้ และเห็นความสำคัญอย่างมาก

6. ข้อเสนอแนะ

ควรมีการวิจัยและพัฒนาระบบเทคโนโลยีสารสนเทศหรือแอปพลิเคชันที่จะนำมาสกัดกั้นปัญหาการกลั่นแกล้งบนโลกไซเบอร์ ที่ครอบคลุมการใช้งานในระดับสถาบันการศึกษาและองค์กรทั่วไปเพื่อให้เกิดแนวทางไปสู่การป้องกันและแก้ไขปัญหาภัยคุกคามและอาชยากรรมทางไซเบอร์ครบวงจร

8. เอกสารอ้างอิง

กุลวดี ราชภักดี. (2545). **ความตระหนักและการปฏิบัติตนเกี่ยวกับการประหยัดพลังงานไฟฟ้าของนักศึกษาในหอพักสถาบันอุดมศึกษา เขตกรุงเทพมหานคร** . สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง. กรุงเทพฯ.

ชฎาภรณ์ สิงห์แก้ว. (2564). บทบาทภาครัฐในการป้องกันอาชญากรรมไซเบอร์เพื่อความมั่นคงทางเศรษฐกิจและสังคม. **วารสารวิชาการมหาวิทยาลัยการจัดการและเทคโนโลยีอิสเทิร์น**. 18(1), น. 9-10.

ชิษณุพงศ์ ธนูทอง. (2557). **การพัฒนาการรักษาความมั่นคงในระบบเครือข่ายหน่วยงานภาครัฐมหาวิทยาลัยธรรมศาสตร์.**

ธานินทร์ ศิลป์จารุ. (2557). **การศึกษาและการวิเคราะห์ข้อมูลทางสถิติ ด้วย SPSS**. กรุงเทพมหานคร: วีอินเตอร์พริ้นท์ กรุงเทพมหานคร.

เมธาพร ธรรมศิริ และศิรภัสสรศ์ วงศ์ทองดี. (2565). ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร. **วารสารวิชาการไทยวิจัยและการจัดการ**. 3(2). หน้า 7.

วาสนา อุทัยแสง. (2559). **การตระหนักรับรู้การบริหารความเสี่ยง และการนำการบริหารความเสี่ยงไปปฏิบัติของบุคลากรมหาวิทยาลัยมหาสารคาม**. กองแผนงาน สำนักงานอธิการบดี. มหาวิทยาลัยมหาสารคาม.

สุธาเทพ รุณเรศ. (2561). **ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร**. การค้นคว้าอิสระ หลักสูตรวิทยาศาสตรมหาบัณฑิตสาขาวิชานโยบายและการบริหารเทคโนโลยีสารสนเทศ วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์.

Cochran, W.G. (1977). **Sampling Techniques**. 3d ed. New York: John Wiley and Sons Inc.

Marketing Oops. (2018). Cyber Security Archives. [Online]. Available : **https://www.marketingoops.com/tag/cyber-security/.**Retrieved December 10, 2022.

Nunnally, J. C. (1978). **Psychometric theory**. (2nd ed.). New York: McGraw Hill Inc.

คุณค่าทางวิชาการ

งานวิจัยนี้ได้นำเสนอการตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ของผู้ใช้งานระบบเครือข่ายอินเทอร์เน็ตในสถานศึกษา จังหวัดสุรินทร์ เพื่อให้ทราบถึงลักษณะประชากรที่ส่งผลต่อความตระหนักรู้ถึงภัยคุกคามและอาชญากรรมไซเบอร์ ระดับประสบการณ์และระดับความรู้ของผู้ใช้งานอินเทอร์เน็ตในสถานศึกษาเพื่อป้องกันภัยคุกคามและอาชญากรรมไซเบอร์ โดยสามารถนำผลจากการวิจัย ไปต่อยอดเพื่อออกแบบการเรียนรู้ที่เหมาะสมเพื่อป้องกันภัยคุกคามและอาชญากรรมไซเบอร์ที่สอดคล้องเหมาะสมกับปัจจุบัน ตามรูปแบบการใช้อินเทอร์เน็ตที่เปลี่ยนแปลงไปอย่างรวดเร็วเพื่อให้ผู้ใช้งานอินเทอร์เน็ตในสถานศึกษารู้เท่าทันและป้องกันตนเองได้ก่อนที่จะเกิดความไม่ปลอดภัยกับชีวิตและทรัพย์สินจากภัยและอาชญากร