# ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562

โดย

พลตรี เอกรัตน์ ช้างแก้ว
รองผู้บัญชาการโรงเรียนนายร้อยพระจุลจอมเกล้า

นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 62
ประจำปีการศึกษา พุทธศักราช 2562 - 2563

# หนังสือรับรอง

วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ได้อนุมัติให้เอกสารวิจัยส่วนบุคคล เรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” ลักษณะวิชาวิทยาศาสตร์และเทคโนโลยีของ พลตรี เอกรัตน์ ช้างแก้ว เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรการป้องกันราชอาณาจักร รุ่นที่ 62 ประจำปีการศึกษา พุทธศักราช 2562 - 2563

พลโท

(พิสัณห์ ปฐมเอม)
ผู้อำนวยการวิทยาลัยป้องกันราชอาณาจักร
สถาบันวิชาการป้องกันประเทศ

# บทคัดย่อ

**เรื่อง** ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562

**ลักษณะวิชา** วิทยาศาสตร์และเทคโนโลยี

**ผู้วิจัย** พลตรี เอกรัตน์ ช้างแก้ว **หลักสูตร วปอ. รุ่นที่** 62

การวิจัยเรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาความเข้าใจภัยคุกคามทางไซเบอร์ ประเมินความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 เพื่อเสนอแนวทางการพัฒนาหลักสูตรการรักษาความปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ และเพื่อเสนอการประยุกต์ใช้ในการพัฒนาบุคลากรของกองทัพบกในการรับมือกับภัยคุกคามทางไซเบอร์ต่อไป

การวิจัยนี้เป็นการวิจัยเชิงปริมาณและการวิจัยเชิงคุณภาพ ประชากร คือ นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าที่กำลังศึกษาในปีการศึกษา 2562 ทุกชั้นปี ขนาดตัวอย่าง 300 นาย โดยให้กลุ่มตัวอย่างกรอกแบบสอบถามด้วยตนเอง

ผลการวิจัยพบว่า ปัจจัยทางด้านชั้นปีการศึกษา มีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ ปัจจัยทางด้านหลักสูตรการศึกษา ไม่มีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ และปัจจัยด้านประสบการณ์ภัยคุกคามทางไซเบอร์ มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562

ผลการวิจัยและการสัมภาษณ์กลุ่มตัวอย่างสามารถนำมาวิจัยเชิงคุณภาพเพื่อหาแนวทางการพัฒนาหลักสูตรวิทยาศาสตรบัณฑิต สาขาความมั่นคงปลอดภัยทางไซเบอร์ ได้แก่ แนวทางการพัฒนาหลักสูตรเพื่อให้สอดคล้องกับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสากล การพัฒนาความรู้พื้นฐานทางเทคโนโลยีสารสนเทศที่จำเป็น การพัฒนาสื่อการเรียนการสอนที่เหมาะสม การพัฒนาอาจารย์ผู้สอน และทักษะที่ควรได้รับจากหลักสูตรฯ

# Abstract

The objective of the research “The Awareness of Cyber Threats among Cadets of Chulachomklao Royal Military Academy in the 2019 Academic Year” is to study and to assess the understanding of cyber threats among cadets at Chulachomklao Royal Military Academy. In addition, this study aims to propose guidelines for developing a cyber security course for cadets, which will enable cadets to cope with cyber threats effectively. The research also discusses the application of these guidelines to the development of Royal Thai Army personnel in response to cyber threats.

This research utilizes both quantitative and qualitative methodology. The population is the cadets of Chulachomklao Royal Military Academy who are studying in the 2019 academic year in every grade with a sample size of 300 cadets.

The research found factors throughout the 2019 academic year that affected the awareness of cyber threats among cadets, including experiences of cyber threats. However, factors related to the educational curriculum had no effect on the awareness of cyber threats.

The guidelines formed as a result of the research findings and sample interviews can be used for further qualitative research to develop a cyber security course for a Bachelor of Science Curriculum. These guidelines should comply with international cyber security standards, the development of essential information technology knowledge, and the development of appropriate teaching materials. In addition, this research can be used to develop teachers and the skills that should be gained from the courses.

# คำนำ

การวิจัยเรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” จัดทำขึ้นตามหลักสูตรการศึกษาของวิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ซึ่งนักศึกษาได้ทำการศึกษาค้นคว้าจากเอกสาร วารสาร อินเทอร์เน็ต และแหล่งข้อมูลต่าง ๆ โดยใช้กระบวนการวิจัยในการค้นคว้า วิเคราะห์ข้อมูล ให้ได้ผลการวิจัยที่เป็นประโยชน์ สามารถนำไปประยุกต์ใช้ให้สอดคล้องกับสถานการณ์ปัจจุบันและเป็นแนวทางในการพัฒนาต่อไปในอนาคต

พลตรี

(เอกรัตน์ ช้างแก้ว)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 62
ผู้วิจัย

# กิตติกรรมประกาศ

งานวิจัยฉบับนี้สำเร็จลงได้ด้วยดี เนื่องจากได้รับความกรุณาอย่างสูงจากผู้บังคับบัญชาและอาจารย์วิทยาลัยป้องกันราชอาณาจักร สถาบันวิชาการป้องกันประเทศ ที่กรุณาให้คำแนะนำปรึกษาตลอดจนปรับปรุงแก้ไขข้อบกพร่องต่าง ๆ ด้วยความเอาใจใส่อย่างดียิ่ง ผู้วิจัยตระหนักถึงความตั้งใจจริงและความทุ่มเทของอาจารย์ และขอขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบคุณนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปีการศึกษา 2562 ที่ให้ความร่วมมือสละเวลาในการตอบแบบสอบถามและสัมภาษณ์ ขอขอบคุณ พันเอก รศ.ดร.อนันต์ ปัจวิทย์ เพื่อนร่วมรุ่นและเพื่อนร่วมงานที่มีความรู้และความสามารถให้คำแนะนำและการสนับสนุนอย่างดีเยี่ยม ขอขอบคุณ พันเอกหญิง ผศ.ภมร จินดามณี ที่ช่วยในการดำเนินการในทุกด้าน ขอบคุณ จ่าสิบเอก ประศาล โยมเรือง และ สิบเอก อนุรักษ์ หรั่งเจริญ ช่วยดำเนินการด้านธุรการและอื่น ๆ จนทำให้งานวิจัยนี้สำเร็จลุล่วงไปด้วยดี และขอขอบคุณ พันเอกหญิง สุกัญญา ช้างแก้ว นางสาว จิรศรี ช้างแก้ว และนายกมลพงศ์ ช้างแก้ว ครอบครัวที่เป็นกำลังใจและอยู่เบื้องหลังในทุกสิ่งเสมอมา

อนึ่ง ผู้วิจัยหวังว่า งานวิจัยฉบับนี้จะมีประโยชน์ต่อผู้เกี่ยวข้องไม่มากก็น้อย ขอมอบส่วนดีทั้งหมดให้กับคณาจารย์ที่ได้ประสิทธิประสาทวิชา และขอมอบความกตัญญูกตเวทิตาคุณแด่บิดา มารดา และผู้มีพระคุณทุกท่าน สำหรับข้อบกพร่องต่าง ๆ ที่อาจเกิดขึ้น ผู้วิจัยขอน้อมรับเพียงผู้เดียว และยินดีจะรับฟังคำแนะนำจากทุกท่านที่ได้เข้ามาศึกษาเอกสารวิจัยฉบับนี้ เพื่อเป็นประโยชน์ในการพัฒนางานวิจัยต่อไป

พลตรี

(เอกรัตน์ ช้างแก้ว)
นักศึกษาวิทยาลัยป้องกันราชอาณาจักร
หลักสูตร วปอ. รุ่นที่ 62
ผู้วิจัย

# สารบัญ

# สารบัญ (ต่อ)

# สารบัญ (ต่อ)

# สารบัญตาราง

# สารบัญตาราง (ต่อ)

# สารบัญแผนภาพ

# สารบัญแผนภาพ (ต่อ)

# บทที่ 1
# บทนำ

## ความเป็นมาและความสำคัญของปัญหา

วิทยาการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ก้าวหน้าไปอย่างรวดเร็วในช่วงสิบปีที่ผ่านมา และยังพัฒนาต่อไปในรูปแบบที่หลากหลายมากขึ้น มีการกระจายไปในทุกระบบของสังคม นำมาซึ่งความสะดวกสบายของผู้คนบนโลกที่เข้าถึงและนำมาประยุกต์เพื่อใช้ประโยชน์กับตนเอง และกับสังคม เศรษฐกิจ การเมือง ความมั่นคง แต่อย่างไรก็ตามความก้าวหน้าและการพัฒนาทางด้านเทคโนโลยีเหล่านี้ก็อาจนำมาซึ่งภัยอันตรายขนาดเล็กระดับบุคคล ครอบครัว องค์กร จนถึงขนาดใหญ่ระดับประเทศหรือระดับโลกได้ ซึ่งรูปแบบของภัยอันตรายที่เปลี่ยนแปลงไปจากเดิมนี้เรียกว่าภัยคุกคามทางไซเบอร์ (Cyber Threats)

ปัจจุบันหน่วยงานต่าง ๆ ได้พยายามป้องกันภัยคุกคามทางไซเบอร์นี้ โดยให้ความสำคัญในการพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) มากขึ้น อาจเพราะเห็นผลร้ายที่เกิดขึ้นทั้งในระดับองค์กรเอง และตัวอย่างจากนอกองค์กรที่เป็นข่าวอยู่บ่อยครั้ง หรือด้วยกฎหมายบังคับให้ต้องปฏิบัติตาม ทำให้มีการพัฒนาเรื่องดังกล่าวไปพอสมควร แต่อย่างไรก็ตามยังต้องมีเรื่องที่ต้องทำความเข้าใจและปรับปรุงให้ดีขึ้น เพื่อให้เท่าทันไปกับรูปแบบของภัยคุกคามที่เปลี่ยนแปลง

สิ่งหนึ่งที่ต้องให้ความสำคัญคือการพัฒนาศักยภาพของบุคลากรในองค์กร เพื่อให้มีความรู้ความเข้าใจในการบริหารจัดการและการใช้เครื่องมือต่าง ๆ ได้อย่างมีประสิทธิภาพ และเป็นไปตามกระบวนการที่เหมาะสม เพราะหากมีการนำมาใช้ไม่ถูกต้อง หรือไม่มีความเข้าใจก็อาจทำให้เกิดความเสียหาย สูญเสียงบประมาณและความคุ้มค่าในการดำเนินการ แต่การจะทำความเข้าใจสิ่งเหล่านี้ได้นั้นต้องมีพื้นฐานความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ เพื่อนำไปประยุกต์ใช้เทคโนโลยีด้านสารสนเทศต่าง ๆ ได้อย่างเหมาะสมให้เกิดความมั่นคงปลอดภัยทางไซเบอร์ ป้องกันความเสียหายต่าง ๆ ที่อาจเกิดขึ้นกับองค์กรได้

โรงเรียนนายร้อยพระจุลจอมเกล้า เป็นหน่วยงานของกองทัพบกที่มีหน้าที่หลักในการผลิตนายทหารสัญญาบัตรให้กับกองทัพบก ผู้บังคับบัญชาของกองทัพบกจึงเล็งเห็นความสำคัญในการพัฒนานักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ให้มีความรู้ ความสามารถด้านไซเบอร์และการรักษาความปลอดภัยทางไซเบอร์ เท่าทันเทคโนโลยีในปัจจุบัน แต่การจะพัฒนาความรู้ด้านไซเบอร์ให้กับนักเรียนนายร้อยได้ จำเป็นต้องทราบพื้นฐานความตระหนักรู้ด้านภัยคุกคามทางด้านไซเบอร์ก่อน เพื่อเป็นแนวทางในการพัฒนาต่อยอดองค์ความรู้ให้กับนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าได้อย่างเหมาะสม ผู้วิจัยจึงได้วิจัยเรื่องความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า เพื่อเป็นการศึกษาพื้นฐานด้านบุคลากรของนายทหารสัญญาบัตรหลักของกองทัพบกในอนาคต ว่ามีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์มากน้อยเพียงใด และมีความพร้อมที่จะรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น ได้อย่างเพียงพอ

หรือไม่ โดยในอนาคตสามารถนำไปใช้ทบทวนในการพัฒนาหลักสูตรความปลอดภัยทางไซเบอร์ให้กับนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าได้อย่างเหมาะสมและมีประสิทธิภาพ เพื่อให้เป็นนายทหารที่มีบทบาทสำคัญในเผยแพร่ความรู้ให้กับกำลังพลในกองทัพ การระวังป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของตนเอง และของหน่วยงานของกองทัพบก และมีศักยภาพในการส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพบกและประเทศชาติต่อไป

## วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาความเข้าใจภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 และแนวทางการรักษาความปลอดภัยทางไซเบอร์ในปัจจุบัน

2. เพื่อวิเคราะห์ประเมินความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

3. เพื่อเสนอแนวทางการพัฒนาหลักสูตรการรักษาความปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

4. เสนอการประยุกต์ใช้ในการพัฒนาบุคลากรของกองทัพบก ในการรับมือกับภัยคุกคามทางไซเบอร์ต่อไป

## ขอบเขตการวิจัย

1. ประชากร นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ที่กำลังศึกษาในปีการศึกษา 2562 จำนวน 1,141 นาย

2. กลุ่มตัวอย่าง นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ชั้นปีที่ 1- 5 ที่กำลังศึกษาในภาคการศึกษาที่ 2 ปีการศึกษา 2562 จำนวน 300 นาย

3. ตัวแปรที่ใช้

3.1 ตัวแปรต้น

3.1.1 ชั้นปีของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

3.1.2 หลักสูตรที่ศึกษา

3.1.3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

3.2 ตัวแปรตาม ความตระหนักรู้ภัยคุกคามทางไซเบอร์

3.2.1 การจารกรรมข้อมูล

3.2.2 โปรแกรมประสงค์ร้าย

3.2.3 สื่อสังคมออนไลน์ที่ไม่เหมาะสม

## วิธีดำเนินการวิจัย

เอกสารวิจัยฉบับนี้เป็นการวิจัยเชิงปริมาณ และเชิงคุณภาพ หรือแบบผสมผสาน (Mixed Method) โดยการทำแบบสอบถามที่ให้ความสำคัญกับมุมมอง ประสบการณ์ และการกระทำของกลุ่มที่ต้องการศึกษา และนำมาวิเคราะห์ เพื่อให้เข้าใจความตระหนักรู้ด้านไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

1. ศึกษาภัยคุกคามทางไซเบอร์ และแนวทางการรักษาความปลอดภัยทางไซเบอร์จากแหล่งเรียนรู้ต่าง ๆ ได้แก่ เอกสาร หนังสือ งานวิจัย และสื่อสารสนเทศออนไลน์

2. ออกแบบแบบทดสอบความตระหนักรู้ภัยคุกคามทางไซเบอร์

3. ทดสอบความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย ชั้นปีที่ 1-5 ที่กำลังศึกษาในภาคการศึกษาที่ 2 ปีการศึกษา 2562 จำนวน 150 นาย

4. ประเมินระดับความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย ชั้นปีที่ 1-5 ที่กำลังศึกษาในภาคการศึกษาที่ 2 ปีการศึกษา 2562 โดยใช้เกณฑ์คะแนน

5. วิเคราะห์ระดับความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย ชั้นปีที่ 1-5 ที่กำลังศึกษาในภาคการศึกษาที่ 2 ปีการศึกษา 2562

6. เสนอแนะแนวทางการพัฒนาหลักสูตร เพื่อให้นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า มีความรู้พื้นฐานทางด้านการรักษาความปลอดภัยทางไซเบอร์

## ระยะเวลาดำเนินการวิจัย

1. การจัดทำโครงการวิจัย ระยะเวลา 15 ต.ค. - 31 ส.ค. 62

2. ทบทวนวรรณกรรม ศึกษาภัยคุกคามและแนวทางการรักษาความปลอดภัยทางไซเบอร์ ระยะเวลา 1 พ.ย.62 - 29 ก.พ.63

3. ออกแบบทดสอบความตระหนักรู้ภัยคุกคามทางไซเบอร์ ระยะเวลา 1 มี.ค.-31 มี.ค.63

4. ประเมินระดับความตระหนักรู้ภัยคุกคามทางไซเบอร์ ระยะเวลา 1 เม.ย.-30 เม.ย.63

5. วิเคราะห์ระดับความตระหนักรู้ภัยคุกคามทางไซเบอร์ ระยะเวลา 1 พ.ค.-15 พ.ค.63

6. สรุปและข้อเสนอแนะ ระยะเวลา 16 พ.ค. - 31 พ.ค.63

7. จัดทำเอกสาร ระยะเวลา 1 ธ.ค.62 - 31 พ.ค.63

## ประโยชน์ที่ได้รับจากการวิจัย

1. ได้ทราบถึงความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

2. ได้แนวทางพัฒนาหลักสูตรการรักษาความปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า เพื่อให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้

3. วิทยาลัยป้องกันราชอาณาจักร มีเอกสารที่เกี่ยวข้องกับความรู้ความเข้าใจสถานการณ์ ภัยคุกคามทางไซเบอร์ และแนวทางการรักษาความปลอดภัยทางไซเบอร์ในปัจจุบัน

4. ผู้บังคับบัญชาและอาจารย์โรงเรียนนายร้อยพระจุลจอมเกล้า สามารถประเมินความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

5. คณะกรรมการกำกับหลักสูตรด้านไซเบอร์ของโรงเรียนนายร้อยพระจุลจอมเกล้า มีแนวทางการพัฒนาหลักสูตรการรักษาความปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

6. แบบประเมินความตระหนักรู้ด้านไซเบอร์ สามารถนำไปใช้ทดสอบอาจารย์ โรงเรียนนายร้อยพระจุลจอมเกล้า กำลังพลของกองทัพบกในหน่วยต่าง ๆ และบุคคลทั่วไปที่สนใจ

7. เพื่อต่อยอดการพัฒนาบุคลากรของกองทัพบกในการรับมือกับภัยคุกคามทางไซเบอร์

## คำจำกัดความ

ไซเบอร์ (Cyber) หมายถึง กิจกรรมที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ระบบคอมพิวเตอร์ การสื่อสารข้อมูลคอมพิวเตอร์ (อ้างอิง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562)

ความปลอดภัยทางไซเบอร์ (Cyber Security)

หมายถึง มาตรการและดำเนินการปกป้อง ป้องกัน ส่งเสริมเพื่อรับมือและแก้ไขสถานการณ์ด้านภัยคุกคามที่จะส่งผลต่อไซเบอร์ โดยเฉพาะการให้บริการด้านระบบเครือข่ายคอมพิวเตอร์อินเทอร์เน็ต โครงข่ายโทรคมนาคม การให้บริการดาวเทียม ระบบกิจการสาธารณูปโภคพื้นฐาน ระบบกิจการสาธารณะสำคัญ ซึ่งเป็นเครือข่ายในระดับประเทศ เพื่อมิให้เกิดผลกระทบต่อความมั่นคงของชาติ ความมั่นคงทางการทหาร ความสงบเรียบร้อยภายในประเทศ และความมั่นคงทางเศรษฐกิจ (อ้างอิงพระราชบัญญัติ การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562)

ความตระหนักรู้ทางไซเบอร์ (Cyber Security Awareness)

หมายถึง การรับรู้ถึงภัยคุกคามทางไซเบอร์ และสามารถป้องกันตนเองได้พื้นฐานความมั่นคงปลอดภัยของไซเบอร์

หมายถึง หลักการพื้นฐานสำคัญในเรื่องความมั่นคงปลอดภัยทางไซเบอร์

# บทที่ 2
# การทบทวนวรรณกรรมที่เกี่ยวข้อง

การศึกษาเรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” ผู้วิจัยได้รวบรวมแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องที่ต้องการศึกษา โดยแนวคิด ทฤษฎี วรรณกรรม และงานวิจัยที่เกี่ยวข้องที่รวบรวมมีดังนี้

1. แนวคิดและทฤษฎีที่เกี่ยวข้องกับความรู้ ทัศนคติ และพฤติกรรม
2. แนวความคิดเกี่ยวกับความตระหนักรู้
3. แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)
4. รูปแบบการรักษาความปลอดภัยทางไซเบอร์
5. ทฤษฎีเกี่ยวกับภัยคุกคามทางไซเบอร์ (Cyber Threats)
6. นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.2562-2565)
7. ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ.2560-2564)
8. การพัฒนาบุคลากรของกองทัพบกในการรับมือกับภัยคุกคามทางไซเบอร์
9. มาตรฐานการรักษาความปลอดภัยทางไซเบอร์ในระดับสากล
10. หลักสูตรของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562
11. พันธกิจของโรงเรียนนายร้อยพระจุลจอมเกล้าในการผลิตนายทหารสัญญาบัตร
12. การพัฒนาหลักสูตรการรักษาปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า
13. งานวิจัยที่เกี่ยวข้อง

## แนวคิดและทฤษฎีที่เกี่ยวกับความรู้ ทัศนคติ และพฤติกรรม

### 1. แนวคิดเกี่ยวกับความรู้

สุรพงษ์ โสธนะเสถียร (2533) กล่าวว่าบุคคลส่วนมากจะรับรู้เบื้องต้นผ่านประสบการณ์ แล้วนำมาจัดระบบเป็นโครงสร้างของความรู้ผสมผสานระหว่างความจำกับสภาพจิตวิทยา ความรู้จึงเป็นความจำที่เลือกสรรให้สอดคล้องกับสภาพจิตใจของตน ซึ่งความรู้ทำให้ผู้เรียนได้รู้ถึงความสามารถในการจำ และรำลึกถึงเหตุการณ์ และประสบการณ์ที่เคยพบมาแล้ว ซึ่งได้แยกการประเมินระดับความรู้ไว้ 6 ระดับ ดังนี้

1. ระดับที่ระลึกได้ (Recall) เป็นระดับที่มีความสามารถในการดึงข้อมูลออกมาจากความจำได้

2. ระดับที่รวบรวมสาระสำคัญได้ (Comprehensive) เป็นระดับที่สามารถทำบางสิ่งบางอย่างได้มากกว่าการจำเนื้อหาที่ได้รับ สามารถเขียนข้อความด้วยถ้อยคำของตนเอง สามารถแสดง

ให้เห็นได้ด้วยภาพ ให้ความหมาย แปลความ และเปรียบเทียบความคิดอื่น ๆ หรือคาดคะเนผลที่เกิดขึ้นต่อไปได้

3. ระดับของการนำไปใช้ (Application) สามารถนำเอาข้อเท็จจริง และความคิดเห็นที่เป็นนามธรรมไปปฏิบัติอย่างเป็นรูปธรรม

4. ระดับการวิเคราะห์ (Analysis) เป็นระดับที่สามารถให้ความคิดในรูปของการนำความคิดมาแยกส่วน เป็นประเภท หรือการนำข้อมูลมาประกอบกันเพื่อปฏิบัติของตนเอง

5. ระดับของการสังเคราะห์ (Synthesis) คือ การนำเอาข้อมูลแนวความคิดมาประกอบแล้วนำไปสู่การสร้างสรรค์ที่ต่างจากเดิม

6. ระดับการประเมิน (Evaluation) คือ ความสามารถในการใช้ข้อมูลเพื่อตั้งเกณฑ์การรวบรวมผล และวัดข้อมูลตามมาตรฐาน เพื่อให้ตั้งข้อตัดสินถึงระดับของประสิทธิผลของกิจกรรมแต่ละอย่าง

สุวรีย์ ศิวะแพทย์ (2549) ความรู้ หมายถึง การได้ข้อมูลเกี่ยวกับข้อเท็จจริง รูปแบบวิธีการ กฎเกณฑ์ แนวปฏิบัติ สิ่งของ เหตุการณ์ หรือบุคคล ซึ่งได้จากการสังเกตุ ประสบการณ์ หรือจากสื่อต่าง ๆ ประกอบกับความรู้จึงเป็นความสามารถในการใช้ข้อเท็จจริงหรือความคิด ความหยั่งรู้หยั่งเห็น หรือสามารถเชื่อมโยงความคิดเข้ากับเหตุการณ์

## 2. แนวคิดเกี่ยวกับทัศนคติ

Rokealth Milton (1972) ให้ความหมายว่าทัศนคติเป็นการผสมผสานและจัดระเบียบความเชื่อของคนเราที่มีต่อสิ่งใดสิ่งหนึ่ง หรือสถานภาพใดสถานภาพหนึ่ง ภาพรวมของความเชื่อเป็นส่วนประกอบในตัวบุคคลซึ่งอาจรู้ตัวหรือไม่รู้ตัวก็ได้ แต่สามารถรู้ได้จากคำพูด การกระทำ ไม่ว่าความเชื่อจะออกมารูปใดก็ตาม ก็จะเป็นส่วนที่กำหนดแนวโน้มของบุคคลในการที่จะกระทำสิ่งใดสิ่งหนึ่ง

Roger (1978) อ้างถึงใน สุรพงศ์ โสธนะเสถียร , 2533) ได้กล่าวถึงทัศนคติว่าเป็นดัชนีชี้ว่าบุคคลนั้น คิดและรู้สึกอย่างไรกับคนรอบข้าง วัตถุหรือสิ่งแวดล้อมตลอดจนสถานการณ์ต่าง ๆ โดยทัศนคตินั้นมีรากฐานมาจากความเชื่อที่อาจส่งผลถึงพฤติกรรมในอนาคต ทัศนคติจึงเป็นความพร้อมที่ตอบสนองต่อสิ่งเร้า และเป็นมิติของการประเมิน เพื่อแสดงว่าชอบหรือไม่ชอบต่อประเด็นหนึ่ง ๆ ซึ่งถือเป็นการสื่อสารภายในบุคคล (Interpersonal Communication) ซึ่งเป็นผลกระทบมาจากการรับสาร อันจะมีผลต่อพฤติกรรมต่อไป

## 3. แนวความคิดเกี่ยวกับพฤติกรรม หรือการมีส่วนร่วม

สุรพงษ์ โสธนะเสถียร (2550) กล่าวว่า “พฤติกรรม คือ การกระทำใด ๆ ของคนเราส่วนใหญ่เป็นการแสดงออกของบุคคล โดยมีพื้นฐานมาจากความรู้และทัศนคติ การที่บุคคลมีพฤติกรรมแตกต่างกันเพราะมีความรู้และทัศนคติที่แตกต่างกัน เกิดขึ้นจากความแตกต่างของการเปิดรับสื่อและความแตกต่างการแปลความสารที่ตนเองได้รับ จึงก่อให้เกิดประสบการณ์สั่งสมที่แตกต่างกัน อันมีผลกระทบต่อพฤติกรรมของบุคคล

อรวรรณ ปิลันะน์โอวาท (2549) กล่าวว่า “การกระทำ หรือพฤติกรรมใด ๆ ของคนส่วนใหญ่ ตามปกติมักเกิดจากทัศนคติของบุคคลนั้น ๆ ทัศนคติจึงเป็นเสมือนเครื่องควบคุมการกระทำของบุคคลพฤติกรรมส่วนใหญ่ของคนถูกควบคุมด้วยทัศนคติของเขา

แนนซี ชวารัตช์ (Nancy E.Schwart) กล่าวถึงการเปลี่ยนพฤติกรรมของคนเราว่ามีความสำคัญระหว่างความรู้ ทัศนคติ และการปฏิบัติรูปแบบ 4 ประการ ดังนี้

1. ทัศนคติเป็นตัวกลางทำให้เกิดการเรียนรู้และการปฏิบัติ ดังนั้นความรู้มีความสัมพันธ์กับทัศนคติ และมีผลต่อการปฏิบัติ

2. ความรู้และทัศนคติมีความสัมพันธ์กันและทำให้เกิดการปฏิบัติตามมา

3. ความรู้และทัศนคติต่างทำให้เกิดการปฏิบัติได้โดยที่ความรู้และทัศนคติไม่จำเป็นต้องมีความสัมพันธ์กัน

4. ความรู้มีผลต่อการปฏิบัติทั้งทางตรงและทางอ้อม

## แนวความคิดเกี่ยวกับความตระหนักรู้

ความตระหนัก (Awareness) เป็นแนวคิดเชิงจิตวิทยา (Phychological Approach) ผสมผสานกับแนวคิดเชิงพฤติกรรมศาสตร์ (Behavior Science) โดยมีหลักการ แนวคิด ทฤษฎีเกี่ยวกับความตระหนักดังนี้

1. ความหมายของความตระหนัก

พจนานุกรมราชบัณฑิตสถาน พ.ศ.2542 ได้ให้ความหมาย “ความตระหนักว่าเป็นการรู้ประจักษ์ชัด รู้ชัดแจ้ง” โดยสอดคล้องกับพจนานุกรมของ Good (1973 : 54) โดยได้ให้ความหมายว่า “การแสดงออกจากการระลึกได้หรือจดจำได้” นอกจากนั้น ยังมีผู้นิยามไว้อีก ดังนี้

กุลวดี ราชภักดี (2545 : 38) กล่าวถึงความตระหนักว่า หมายถึง ภาวการณ์ที่บุคคลเกิดความรู้สึกนึกคิด ความคิดเห็นหรือประสบการณ์จากเหตุการณ์ใดเหตุการณ์หนึ่ง เป็นภาวะที่บุคคลเข้าใจและประเมินสถานการณ์ที่เกี่ยวข้องกับตนเองได้ โดยเกิดจากสภาวะจิตที่ยอมรับหรือภาวการณ์หรือความโน้มเอียงที่จะเลือกพฤติกรรม และปฏิบัติตนเพื่อแสดงต่อปัญหาหรือเหตุการณ์หนึ่งที่ได้ประสบ

เริงขัย คงสงค์ (2547) กล่าวว่าความตระหนักเป็นสภาวะทางจิตใจที่เกี่ยวกับความสำนึก ความรู้สึก นึกคิด และความปรารถนาของบุคคลต่อสิ่งหนึ่งสิ่งใด หรือเหตุการณ์ใดเหตุการณ์หนึ่ง โดยมีเหตุการณ์สภาพแวดล้อมสังคมหรือสิ่งเร้าจากภายนอกเป็นปัจจัยที่ทำให้บุคคลเกิดความตระหนัก

เกษม จันทร์แก้ว (2547) กล่าวว่าความตระหนัก หมายถึง การที่บุคคลหนึ่งได้ฉุกคิด หรือเกิดความรู้สึกว่าสิ่งใดสิ่งหนึ่ง หรือเหตุการณ์ใดเหตุการณ์หนึ่ง ภายใต้สภาวะจิตใจที่สามารถแสดงออก ด้วยการพูด การเขียน การอ่านหรืออื่น ๆ โดยอาศัยระยะ เวลา ประสบการณ์ หรือสภาพแวดล้อมทางสังคม หรือสิ่งเร้าจากภายนอกให้เกิดความรู้สึกจากการสัมผัส การรับรู้ ความคิดรวบยอด การเรียนรู้ หรือความรู้ ส่งผลให้เกิดความตระหนักและนำไปสู่พฤติกรรมแสดงออกในสิ่งนั้น

กุลวดี สุดหล้า (2550) กล่าวว่าความตระหนัก หมายถึง การแสดงออกซึ่งความรู้สึก ความเห็น ความสำนึก เป็นภาวะที่บุคคลเข้าใจและประเมินสถานการณ์ที่เกิดขึ้นเกี่ยวกับตนเองได้โดยอาศัย ระยะเวลา เหตุการณ์ ประสบการณ์ หรือสภาพแวดล้อมเป็นปัจจัยทำให้เกิดความตระหนัก

นงลักษณ์ วงศ์ถนอม (2548 : 51) กล่าวถึงความตระหนักว่า หมายถึง ความสำนึกที่บุคคลเคยมีความรู้สึกนึกคิดที่เกิดขึ้นในสภาวะจิตใจต่อเหตุการณ์หนึ่งที่ได้ประสบ แล้วแสดงความรู้สึกออกมาทางพฤติกรรม

ประพล มิลินทจินดา (2542 : 19) ได้ให้นิยามว่า “ความตระหนัก คือ การแสดงความรู้สึก นึกคิด ความคิดเห็น ที่บุคคลเข้าใจและประเมินสถานการณ์ที่เกิดขึ้นเกี่ยวกับตนเองจากประสบการณ์ จากช่วงระยะเวลา จากเหตุการณ์ และจากสภาพแวดล้อม เป็นปัจจัยทำให้มนุษย์มีความตระหนัก”

วีระชน ขาวผ่อง (2551 : 2) ได้ให้นิยามว่า “ความตระหนัก คือ สภาวการณ์มีผลให้เกิดความรู้สึก การรับรู้มุ่งสู่สภาวะจิตแห่งตนคือ ทัศนคติ ความคิด ความเชื่อ ความสนใจ อันจะก่อให้เกิดความตระหนักและจิตสำนึก”

พงษ์ชัย เฉลิมกลิ่น (2551 : 50) ได้ให้นิยามว่า “ความตระหนัก คือ พฤติกรรมที่แสดงถึงความรับผิดชอบต่อสิ่งให้สิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่ง ซึ่งเป็นอารมณ์ความรู้สึกด้านทัศนคติ ค่านิยม ความชอบหรือไม่ชอบ ดีหรือไม่ดี ที่ได้จากการประเมินสิ่งต่าง ๆ ของบุคคลนั้น”

อนุสรณ์ กาลดิษฐ์ (2548 : 51) กล่าวถึงความตระหนักว่า หมายถึง ความสำนึกซึ่งบุคคลเคยมีการรับรู้หรือเคยมีความรู้มาก่อน เมื่อมีสิ่งเร้ามากระตุ้นจึงเกิดความสำนึกหรือความตระหนักขึ้น ความตระหนักมีความหมายเหมือนกับความสำนึก เป็นสภาวะทางจิตใจที่เกี่ยวข้องกับความรู้สึก ความคิด ความปรารถนาต่าง ๆ อันเกิดจากความรู้และความสำนึกต่าง ๆ มาแล้ว โดยมีการประเมินค่าและตระหนักถึงความสำคัญของตนที่มีต่อสิ่งนั้น

Bloom (1971: 271 อ้างถึงใน สุพัตรา ถนอมวงศ์, 2551 : 10) ได้ให้นิยามว่า “ความตระหนักคือ ภาคต่ำสุดทางภาคอารมณ์ซึ่งความตระหนักไม่จำเป็นต้องเน้นปรากฏการณ์หรือสิ่งหนึ่งสิ่งใด แต่ความตระหนักจะเกิดขึ้นเมื่อมีสิ่งเร้าให้เกิดความตระหนัก”

ทั้งนี้สามารถสรุปได้ว่า ความตระหนัก (Awareness) คือ การรับรู้แบบฉุกคิดขึ้นมากะทันหันต่อสิ่งใดสิ่งหนึ่งหรือเหตุการณ์ใดเหตุการณ์หนึ่งซึ่งเป็นอารมณ์ความรู้สึกโดยอาศัยองค์ประกอบจากสิ่งแวดล้อม ประสบการณ์ และสิ่งที่ส่งผลกับอารมณ์ความรู้สึก

2. ปัจจัยที่ทำให้เกิดความตระหนัก

กระบวนการเกิดความตระหนักมาจากกระบวนการทางปัญญา (Cognitive process) ทั้งนี้เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้าหรือรับสัมผัสจากสิ่งเร้าหรือประสบการณ์แล้วจะเกิดการรับรู้จากนั้นจะเข้าใจในสิ่งเร้านั้น และเกิดเป็นความคิดรวบยอด และทำให้มีความรู้ (Knowledge) และเมื่อมีความรู้ในสิ่งนั้นก็จะนำไปสู่การเกิดความตระหนัก ทั้งนี้ความรู้และความตระหนักนี้ต่างก็นำไปสู่การกระทำ (Action) หรือการแสดงพฤติกรรมของบุคคลต่อสิ่งเร้านั้น ๆ

พจนานุกรม ของ Good (1973) ได้ประมวลขั้นตอนของกระบวนการเกิดความตระหนัก ดังนี้ (Good, 1973 อ้างถึงใน สุธาสินี อินทร์ผูก, 2548)

ในลักษณะเช่นนี้ความตระหนักจึงเป็นผลของกระบวนการทาง กล่าวคือ เมื่อบุคคลได้รับการกระตุ้นจากสิ่งเร้า หรือรับสัมผัสจากสิ่งเร้าแล้วเกิดการรับรู้ขึ้นแล้วนำไปสู่การเกิดความเข้าใจในสิ่งเร้านั้น และนำไปสู่การเรียนรู้ขั้นต่อไป และเมื่อบุคคลเกิดมีความรู้ในสิ่งนั้นแล้วนำไปสู่ความตระหนักในที่สุด ซึ่งทั้งความรู้และความตระหนักจะนำไปสู่การกระทำหรือพฤติกรรมของบุคคล

ที่มีต่อสิ่งเร้านั้น ๆ ต่อไป และจากการศึกษาของ ทนงศักดิ์ ประสบกิตติคุณ (ม.ป.ป. อ้างถึงใน พัฒน บุบผาสวรรณ, 2546) กล่าวถึง ปัจจัยทางพฤติกรรมศาสตร์ที่มีผลต่อความตระหนักประกอบด้วย ประสบการณ์ต่อการรับรู้ ความเคยชินต่อสภาพแวดล้อมนั้นก็จะทำให้บุคคลนั้นไม่ตระหนักต่อสิ่งที่เกิดขึ้น ความใส่ใจและการให้คุณค่า ถ้ามนุษย์มีความใส่ใจในเรื่องใดมากก็จะมีความตระหนักในเรื่องนั้นมาก ลักษณะรูปแบบของสิ่งเร้า ถ้าสิ่งเร้านั้นสามารถทำให้ผู้พบเห็นเกิดความสนใจย่อมทำให้ผู้พบเห็นเกิดการรับรู้และความตระหนักขึ้นระยะเวลาและความถี่ในการรับรู้ ถ้ามนุษย์ได้รับรู้บ่อยครั้งเท่าใดก็ยิ่งทำให้มีโอกาสเกิดความตระหนักได้มากขึ้นท่านั้น

สำหรับวิธีการสร้างความตระหนักทำได้ด้วยวิธีต่อไปนี้

1. การเผยแพร่ข้อมูล
2. สร้างข้อความที่มีผลกระทบสูง หรือข้อความกระตุ้นอารมณ์
3. สร้างข้อความที่เชื่อมต่อทัศนคติกับพฤติกรรมที่ผ่านมา

อย่างไรก็ตาม ลักษณะเฉพาะของแต่ละบุคคลมีผลต่อการรับรู้และเกิดความตระหนักที่มุ้งเน้นการเปลี่ยนแปลงการรับรู้เกี่ยวกับกลุ่มหรือต่อวัตถุ รวมทั้งจะเกิดความตระหนักต่อสถานการณ์ที่ส่งเสริมการเปลี่ยนแปลงทัศนคติต่างกัน

3. องค์ประกอบที่ก่อให้เกิดความตระหนัก

เบรกเลอร์ (1986:5) ได้กล่าวไว้ว่า ความตระหนักเกิดจากทัศนคติที่มีต่อสิ่งเร้า อันได้แก่ บุคคล สถานการณ์ กลุ่มสังคม และสิ่งต่างๆ ที่โน้มเอียงหรือที่จะตอบสนองในทางบวกหรือทางลบเป็นสิ่งที่เกิดจากการเรียนรู้และประสบการณ์ โดยองค์ประกอบสำคัญที่ก่อให้เกิดความตระหนักมีอยู่ด้วยกัน 4 ประการ ดังนี้

1. ความรู้ความเข้าใจ (Cognitive Component) จะเริ่มต้นจากระดับง่ายและมีการพัฒนาเพิ่มมากขึ้นตามลำดับ
2. อารมณ์ความรู้สึก (Affective Component) เป็นความรู้สึกด้านทัศนคติ ค่านิยม ความตระหนักชอบหรือไม่ชอบ ดีหรือไม่ดี เป็นองค์ประกอบในการประเมินสิ่งเร้าต่าง ๆ
3. พฤติกรรม (Behavioural Component) เป็นการแสดงออกทั้งทางวาจา กิริยาท่าทางที่มีต่อสิ่งเร้า หรือแนวโน้มที่บุคคลจะกระทำ
4. ขั้นตอนและกระบวนการเกิดความตระหนัก

## แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NTSD) ให้ความหมายของไซเบอร์ (Cyber) ว่าเป็นคำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเตอร์เน็ต (Internet) และยังมีการให้ความหมาย “สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง” (www.ntsd.or.th, 2557)

โดยรวมแล้ว (Cyber) จึงเป็นความหมายเชิงนามธรรม หมายถึง ขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ ซึ่งจะครอบคลุมมากกว่าคอมพิวเตอร์ ซึ่งมีความหมายในเชิงนามธรรมของอุปกรณ์ระบบคอมพิวเตอร์ทั่วไป

ตามพจนานุกรม Cyberspace Operations Lexicon ของกระทรวงกลาโหมสหรัฐอเมริกา กำหนดให้ Cyber Security คือกระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความมั่นคงปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ) ความมั่นคงปลอดภัยของระบบเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่ออาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่าง ๆ (www.enwikipedia.org, 2557)

ความเสี่ยงของ Cyber Security อาจรวมถึงสิ่งต่าง ๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้มีส่วนได้เสีย (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น การรบกวนการทำงานหรือการดำเนินธุรกรรม ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และส่งผลกระทบต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

สหภาพโทรคมนาคมระหว่างประเทศ (International Telecommunication Union) ได้ให้ความหมายของคำว่า ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ว่าคือภาพรวมของเครื่องมือ (Tools) , นโยบาย (Policies) , แนวคิดการรักษาความปลอดภัย (Security concepts), การรักษาความปลอดภัย (Security Safeguards) , แนวทาง (Guidelines) , วิธีการบริหารความเสี่ยง (Risk management), การปฏิบัติ (Actions), การอบรม (Training), วิธีปฏิบัติที่เป็นเลิศ (Best practices), การรับประกัน (Assurance) และเทคโนโลยี (Technologies) ที่สามารถปกป้องสภาพแวดล้อมทางไซเบอร์องค์กร และสินทรัพย์ของผู้ใช้งาน ได้แก่ อุปกรณ์สำหรับเชื่อมต่อคอมพิวเตอร์ ข้อมูลส่วนตัว โครงสร้างพื้นฐาน แอปพลิเคชัน บริการ ระบบสารสนเทศ และภาพรวมของการส่งผ่านหรือเก็บข้อมูลในไซเบอร์ ( www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx)

สำหรับประเทศไทยยังไม่มีนิยามคำว่าความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) ที่ชัดเจน วารสารสถาบันวิชาการป้องกันประเทศ ได้ให้คำนิยามคำว่า ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) คือกระบวนการหรือการกระทำทั้งหมดที่จำเป็นเพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความปลอดภัยของข้อมูลข่าวสาร (Information) ในทุกรูปแบบ รวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม และความผิดพลาดต่าง ๆ โดยควรคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล หรือ CIA 3 ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 มาตรา 3 ได้ให้ความหมายของ “ความมั่นคงปลอดภัยทางไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกันรับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอก

ประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยในประเทศ (www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF)

## รูปแบบของการรักษาความปลอดภัยทางไซเบอร์

การรักษาความปลอดภัยทางไซเบอร์ ได้มีวิวัฒนาการเช่นเดียวกับเทคโนโลยีอื่น ๆ การเรียนรู้และเข้าใจวิวัฒนาการนี้ จะช่วยให้เข้าใจระบบการรักษาความปลอดภัยที่มีอยู่ในปัจจุบันได้ โดยการรักษาความปลอดภัยทางไซเบอร์ ประกอบด้วยการรักษาความปลอดภัยในด้านต่าง ๆ ดังนี้

### 1. การรักษาความปลอดภัยด้านกายภาพ (Physical Security)

ในอดีตที่ผ่านมาทรัพย์สินจะอยู่ในรูปของวัตถุที่จับต้องได้ ข้อมูลที่สำคัญก็จัดเก็บอยู่ในวัตถุเช่นเดียวกัน เนื่องจากข้อมูลถูกบันทึกไว้บนแผ่นหิน แผ่นหนัง แผ่นกระดาษ และบุคคลสำคัญในอดีตส่วนใหญ่จะไม่นิยมบันทึกข้อมูลสำคัญมาก ๆ บนสื่อถาวร เช่น แผ่นหนังหรือกระดาษ และจะไม่สนทนาเกี่ยวกับข้อมูลเหล่านี้กับบุคคลอื่น นอกจากบุคคลที่ไว้ใจได้เท่านั้น ซึ่งอาจเป็นที่มาของคำว่า “ความรู้คืออำนาจ (Knowledge is power) ซึ่งหมายความว่า ผู้ที่มีความรู้ คือ ผู้ที่มีอำนาจนั่นเอง และนี่อาจเป็นรูปแบบการรักษาความปลอดภัยที่ดีที่สุดในตอนนั้น ซุนวู นักปรัชญาชาวจีน ได้กล่าวไว้ว่า “ความลับที่รู้โดยคนมากกว่าหนึ่งคนก็ไม่ถือว่าเป็นความลับอีกต่อไป” การที่จะปกป้องทรัพย์สินที่เป็นวัตถุนั้นก็ต้องใช้การปกป้องทางด้านกายภาพ เช่น กำแพง ปราสาท หรือยาม เป็นต้น

ถ้าต้องมีการส่งข้อมูลไปที่อื่นก็จะใช้ผู้ส่งข่าวและส่วนใหญ่ก็จะมีผู้คุ้มกันติดตามไปด้วย ภัยอันตรายนั้นจะอยู่ในรูปแบบทางกายภาพทั้งสิ้น ไม่มีทางที่จะได้ข้อมูลมาได้ โดยที่ไม่ได้คว้ามาด้วยมือส่วนใหญ่ทรัพย์สิน เช่น เงินทอง หรือข้อมูลที่บันทึกลงบนสื่อจะถูกขโมย หรือแย่งไปจากเจ้าของ

### 2. การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)

การรักษาความปลอดภัยเฉพาะทางด้านกายภาพด้านเดียวนั้น มีจุดอ่อนกล่าวคือ ถ้าข้อมูลถูกขโมยระหว่างการรับส่ง ศัตรูก็สามารถเปิดอ่านและเข้าใจข้อมูลนั้นได้ทันที จนกระทั่งเมื่อยุคของจูเลียส์ ซีซาร์ ข้อบกพร่องนี้ได้มีการคิดค้นวิธีการซ่อนข้อมูล หรือเข้ารหัสข้อมูล (Encryption) ซึ่งข้อมูลจะถูกเข้ารหัสก่อนที่จะส่งให้อีกฝ่ายหนึ่ง ดังนั้นถ้ามีการขโมยข้อมูลระหว่างทาง ผู้อ่านก็จะไม่เข้าใจข้อมูลถ้าไม่รู้วิธีถอดรหัส

แนวความคิดนี้ถูกพัฒนามาใช้ในช่วงสงครามโลกครั้งที่ 2 โดยเยอรมันใช้เครื่องมือที่เรียกว่า “เอ็กนิกมา (Enigma)” สำหรับเข้ารหัสข้อมูลที่รับส่งระหว่างหน่วยทหาร ในขณะนั้นเยอรมันเชื่อว่าไม่มีใครสามารถถอดรหัสได้ ซึ่งต่อมาฝ่ายพันธมิตรก็สามารถถอดรหัสนี้ได้สำเร็จ แต่อย่างไรก็ตามฝ่ายพันธมิตรไม่ได้ใช้ปฏิบัติการทางทหารเพื่อป้องกันทุกครั้ง ทำให้เกิดความเสียหายเกิดขึ้นบ้าง แต่ก็เป็นการป้องกันไม่ให้ฝ่ายเยอรมันรู้ว่ารหัสนั้นถูกถอดรหัสได้แล้ว

### 3. การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

การพัฒนาคอมพิวเตอร์เพื่อให้ใช้งานได้ง่ายและสะดวกมากขึ้น ทำให้บุคคลทั่วไปมีคอมพิวเตอร์ใช้งาน และจัดเก็บข้อมูลในเครื่องนั้นด้วย อาจเกิดความไม่ปลอดภัยในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์

ในช่วงต้นทศวรรษ 1970 เดวิด เบลล์ และลีโอนาร์ด พาดูลา ได้พัฒนาแม่แบบสำหรับการรักษาความปลอดภัยของคอมพิวเตอร์ แม่แบบนี้พัฒนามาจากแนวคิดในการจัดระดับความปลอดภัยข้อมูลของรัฐบาลสหรัฐฯ ซึ่งแบ่งออกได้เป็น 4 ชั้น คือ ไม่ลับ ลับ ลับมาก และลับที่สุด (Unclassified , Confidential , Secret , Top Secret) และระดับสิทธิ์ของผู้ที่เข้าถึงข้อมูลลับนี้ (Clearance) ซึ่งมี 4 ระดับ เหมือนกัน หลักการของระบบนี้คือ ผู้ที่สามารถเข้าถึงข้อมูลในระดับใดระดับหนึ่งได้จะต้องมีสิทธิ์ (Clearance) เท่ากับหรือสูงกว่าชั้นความลับของข้อมูลนั้น ดังนี้ผู้ที่มีสิทธิ์น้อยกว่าชั้นความลับของไฟล์ก็จะไม่สามารถเข้าถึงไฟล์นั้นได้

แนวคิดนี้ได้ถูกนำมาใช้ในกระทรวงกลาโหมของสหรัฐอเมริกา โดยใช้ชื่อว่า มาตรฐาน 5200.28 หรือ TCSEC (Trusted Computing System Evaluation Criteria) หรือเป็นที่รู้จักทั่วไปว่า ออเรนจ์บุ๊ค (Orange Book) ในมาตรฐานนี้ได้กำหนดระดับความปลอดภัยของคอมพิวเตอร์ออกเป็นระดับต่าง ๆ ดังนี้

D : Minimal Protection or Unrated

C1 : Discretionary Security Protection

C2 : Controlled Access Protection

B1 : Labeled Security Protection

B2 : Structured Protection

B3 : Security Domains

A1 : Vetified Design

ในแต่ละระดับออเรนจ์บุ๊คได้กำหนดฟังก์ชันต่าง ๆ ที่ระบบต้องมีและการประกัน ดังนั้น ระบบที่ต้องการใบรับรองว่าจัดอยู่ระดับใด ระบบนั้นต้องมีฟังก์ชันต่าง ๆ ที่กำหนดในระดับนั้น พร้อมทั้งการรับประกันในระดับนั้นได้ด้วย ข้อกำหนดเกี่ยวกับการรับประกันสำหรับระบบเพื่อให้เป็นไปตามมาตรฐานนั้น ต้องใช้เวลาและค่าใช้จ่ายสูงสำหรับผู้ผลิต เป็นผลให้ระบบคอมพิวเตอร์มีเพียงไม่กี่ระบบที่ได้ใบรับรองเหนือกว่าระดับ C2

หลังจากนั้นได้มีการกำหนดมาตรฐานใหม่ขึ้นมาแทนออเรนจ์บุ๊ค เพื่อแก้ข้อบกพร่องในเรื่องเวลาที่ใช้ในการตรวจทดสอบ เพื่อออกใบรับรอง เช่น German Green Book (1989) , Canadian Criteria (1990) , ITSEC : Information Technology Security Evaluation Criteria (1991) และ Federal Criteria (1992) ซึ่งแต่ละมาตรฐานที่กล่าวมานี้ก็เพื่อกำหนดกระบวนการในการออกใบรับรองว่าระบบคอมพิวเตอร์นั้นมีความปลอดภัยระดับไหน อย่างไรก็ตามคอมพิวเตอร์มีวิวัฒนาการอย่างรวดเร็ว ระบบปฏิบัติการสมัยใหม่และฮาร์ดแวร์ใหม่ ๆ ได้ถูกพัฒนาขึ้นมาแทนที่ระบบเก่าเร็วกว่าก่อนที่ระบบเก่าจะได้ใบรับรอง

โดยในปัจจุบัน การนำโทรศัพท์มาใช้ในการเก็บข้อมูล และการประมวลผลด้วยการใช้แอพพลิเคชั่นต่าง ๆ บนโทรศัพท์ มีจำนวนมากและเพิ่มขึ้นอย่างต่อเนื่อง ทำให้นอกจากต้องคำนึงถึงด้านความปลอดภัยของคอมพิวเตอร์แล้ว ยังควรให้ความสำคัญกับความปลอดภัยเกี่ยวกับโทรศัพท์เคลื่อนที่เช่นเดียวกัน

### 4. การรักษาความปลอดภัยเครือข่าย (Network Security)

เมื่อมีการนำคอมพิวเตอร์มาเชื่อมต่อเข้าด้วยกันเข้าเป็นเครือข่าย การเข้ารหัสที่เครื่องคอมพิวเตอร์เครื่องเดียวจึงทำไม่ได้ ซึ่งออเรนจ์บุ๊กไม่ได้มีข้อกำหนดเกี่ยวกับเครือข่ายคอมพิวเตอร์ จึงได้มีการจัดทำมาตรฐาน TNI (Trust Network Interpretation) หรือที่รู้จักกันในนามของเรดบุ๊ก (Red Book) ซึ่งเรดบุ๊กมีข้อกำหนดที่มาจากออเรนจ์บุ๊กทั้งหมดและได้เพิ่มในส่วนของเครือข่ายเข้าไป

### 5. การรักษาความปลอดภัยของข้อมูล (Information Security)

การจะบอกได้ว่าข้อมูลนั้นมีความปลอดภัยหรือไม่ โดยการวิเคราะห์คุณสมบัติ 3 ด้าน ที่เรียกว่า CIA Tread ประกอบด้วย ความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ถ้าขาดคุณสมบัติข้อใดข้อหนึ่งถือว่าข้อมูลนั้นไม่มีความปลอดภัย ดังนั้นระบบรักษาความปลอดภัยข้อมูลจึงเป็นระบบที่ต้องปกป้องรักษาคุณสมบัติทั้ง 3 ด้านของข้อมูล ดังนี้

1. ความลับของข้อมูล (Confidentiality) การรักษาความลับของข้อมูล หมายถึง การทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือการปกป้องข้อมูลไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้

ความต้องการในการรักษาความลับของข้อมูลนั้นเริ่มจาก ด้านการทหารที่ต้องการปกปิดข้อมูลเกี่ยวกับกองทัพไม่ให้ฝ่ายตรงข้ามทราบ เช่น ที่ตั้งหน่วยทหาร แผนการโจมตี จำนวนกำลังพล และอาวุธที่ใช้เป็นต้น ต่อมาหลักการนี้ได้นำมาประยุกต์ใช้ในด้านธุรกิจ เช่น บริษัทผู้ผลิตสินค้าอาจต้องการที่จะเก็บข้อมูลเกี่ยวกับผลิตภัณฑ์ของตัวเองให้เป็นความลับ

กลไกหนึ่งที่ใช้ในการรักษาความลับคือ การเข้ารหัสข้อมูล (Cryptography หรือ Encryption) ซึ่งเป็นการจัดเก็บข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านหรือเข้าใจได้ถ้าไม่รู้วิธีการและคีย์ในการเข้าและถอดรหัส (Key) หรือรหัสผ่าน (Password) เป็นกุญแจที่จะใช้สำหรับการเข้าและถอดรหัสข้อมูลได้

2. ความถูกต้องของข้อมูล (Integrity) หมายถึง ความถูกต้องเชื่อถือได้ของข้อมูลหรือแหล่งที่มา เป็นการป้องกันไม่ให้ข้อมูลถูกเปลี่ยนแปลงจากสภาพเดิม หรือการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเปลี่ยนแปลงข้อมูลได้ ความคงสภาพข้อมูลประกอบด้วย 2 ส่วนคือ ความถูกต้องของเนื้อหาข้อมูล และความถูกต้องของแหล่งที่มาของข้อมูล

3. ความพร้อมใช้งาน (Availability) หมายถึงความสามารถในการใช้ข้อมูลหรือพร้อมใช้ทรัพยากรเมื่อต้องการความพร้อมใช้งานนั้นเป็นส่วนหนึ่งของความมั่นคงของระบบ (Reliability) เนื่องเพราะการที่ระบบไม่พร้อมใช้งานเปรียบเสมือนการไม่มีระบบใช้งาน เช่น การโจมตีแบบทำให้ระบบความต้องการ (Denial of Service : Dos) โดยการเข้าใช้งานระบบพร้อมกันจำนวนมากในเวลาเดียวกัน ทำให้เครื่องแม่ข่ายไม่สามารถทำงานได้ทัน จนเหมือนกับการปฏิเสธการให้บริการ

จากในอดีตที่ผ่านมา ยังไม่สามารถสรุปได้ว่าวิธีการใดสามารถแก้ไขปัญหาเกี่ยวกับการรักษาความปลอดภัยได้ทั้งหมด เพราะการรักษาความปลอดภัยที่ดีนั้นต้องใช้ทุกวิธีการที่กล่าวมาร่วมกัน การรักษาความปลอดภัยทางด้านกายภาพเป็นวิธีการที่ดีสำหรับการปกป้องทรัพย์สิน

ที่เป็นวัตถุ การรักษาความปลอดภัยทางด้านการสื่อสาร (COMSEC) เป็นวิธีการใช้ปกป้องข้อมูลในระหว่างการสื่อสาร การรักษาความปลอดภัยคอมพิวเตอร์ (COMPSEC) เป็นสิ่งจำเป็นสำหรับการเข้าถึงระบบคอมพิวเตอร์ และการรักษาความปลอดภัยเครือข่าย (NETSEC) เป็นสิ่งจำเป็นสำหรับการควบคุมการใช้งานเครือข่าย และวิธีการทั้งหมดนี้ก็เพื่อให้บริการการรักษาความปลอดภัยของข้อมูล (INFOSEC)

## ทฤษฎีเกี่ยวกับภัยคุกคามทางไซเบอร์

1. ภัยคุกคามทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์ พ.ศ. 2562 มาตรา 3 หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้ระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ มุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง (www.ratchakitcha.soc.go.th/DATA/PDF/2562/A/069/T_0020.PDF)

2. ประเภทของภัยคุกคาม

ศูนย์ประสานงานความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย - ไทยเซิร์ต (Thailand Computer Emergency Response Team – ThaiCERT) เป็นหน่วยงาน ในการกำกับดูแลของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์กรมหาชน) (สพธอ.) ซึ่งมีภาระหน้าที่หลักในการตอบสนองและจัดการกับเหตุการณ์ความมั่นคงปลอดภัยคอมพิวเตอร์ (Incident Response) ให้การสนับสนุนที่จำเป็น และให้คำแนะนำในการแก้ไขภัยคุกคามความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ รวมทั้ง ติดตาม และเผยแพร่ข่าวสารและเหตุการณ์ด้านความมั่นคงปลอดภัยทางด้านคอมพิวเตอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้คอมพิวเตอร์และเครือข่ายอินเทอร์ ได้แบ่งประเภทภัยคุกคามทางไซเบอร์เป็น 9 ประเภท ตามที่ได้กำหนดโดย The European Computer Security Incident Response Team (CSIRT) ซึ่งเป็นทีมจัดการปัญหาด้านความปลอดภัยคอมพิวเตอร์ หรือทีมสำหรับรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ ซึ่งหมายถึง กลุ่มหรือคณะบุคคลที่ทำการ , ประสานงาน , และสนับสนุน การตอบสนองต่อเหตุการณ์ละเมิดความปลอดภัยคอมพิวเตอร์และเครือข่าย (เหตุการณ์) ที่เกิดขึ้นภายใน Sites ของผู้ให้บริการของ CSIRT นั้น เช่น การแจ้งเตือน การให้คำแนะนำ การอบรม และการบริหารจัดการ ในสหภาพยุโรป ได้แบ่งประเภทของภัยคุกคามเป็น 9 ประเภทดังนี้

2.1 เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) ภัยคุกคามที่เกิดจากการใช้เผยแพร่ ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมล์ ที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ

2.2 การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) ภัยคุกคามที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้

ตามปกตินั้น มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ ภัยคุกคามอาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DOS (Denial of Service) แบบต่าง ๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคาร สถานที่ ระบบไฟฟ้า ระบบปรับอากาศ

2.3 การฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud) ภัยคุกคามที่เกิดจากการฉ้อฉล ฉ้อโกง หรือการหลอกลวงเพื่อผลประโยชน์ สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาต เพื่อแสวงหาผลประโยชน์ของตนเอง หรือขายสินค้าหรือซอฟแวร์ที่ละเมิดลิขสิทธิ์

2.4 ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) ภัยคุกคามที่เกิดจากความพยายามในการรวบรวมข้อมูลจุดอ่อนของระบบของผู้ไม่ประสงค์ดี (Scanning) ด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟแวร์ที่ติดตั้งหรือการใช้งานข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบเป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรระบบเครือข่าย (Sniffer) เป็นโปรแกรมเล็ก ๆ ที่สร้างขึ้นเพื่อลักลอบดักข้อมูลที่ส่งผ่านเครือข่าย เช่น รหัสผ่าน ข้อมูลทางการเงิน หรือข้อมูลอื่น ๆ ที่ต้องการและการล่อลวงหรือใช้เล่ห์กลต่าง ๆ ให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)

2.5 การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) ภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (Unauthorized Access) หรือเปลี่ยนแปลงแก้ไขข้อมูล (Unauthorized modification) ได้

2.6 ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts) ภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ทั้งที่ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE-Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหว่ใหม่ที่ยังไม่เคยพบมาก่อน เพื่อจะได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบภัยคุกคามนี้รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกคำ (Brute Force)

2.7 การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) ภัยคุกคามเกิดกับระบบที่ถูกบุกรุก /เจาะเข้าระบบได้สำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

2.8 โปรแกรมไม่พึงประสงค์ (Malicious Code) ภัยคุกคามที่เกิดจากโปรแกรมหรือซอฟแวร์ที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพท์ที่ไม่พึงประสงค์ กับผู้ใช้งานหรือระบบ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟแวร์ประสงค์ร้ายนี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟแวร์ประสงค์ร้ายประเภทนี้ ต้องอาศัยผู้ใช้งานเป็นผู้เปิดโปรแกรมหรือซอฟแวร์ก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus , Worm, Trojan หรือ Spyware ต่าง ๆ

2.9 ภัยคุกคามอื่น ๆ นอกเหนือจากที่กำหนดไว้ข้างต้น (Other) ภัยคุกคามประเภทอื่นๆ นอกเหนือจากที่กำหนดไว้ข้างต้น ระบุไว้เพื่อเป็นตัวชี้วัดถึงภัยคุกคามประเภทใหม่หรือไม่สามารถจัดประเภทได้ตามที่ระบุไว้ข้างต้น โดยถ้าจำนวนภัยคุกคามอื่น ๆ ในข้อนี้มีจำนวนมากขึ้น แสดงถึงความจำเป็นที่จะต้องปรับปรุงการจัดแบ่งประเภทภัยคุกคามนี้ใหม่ (www.thaicert.or.th/papers/general/2012/pa2012ge001.html)

จากการรวบรวมสถิติภัยคุกคามทางไซเบอร์ประจำปี 2562 ในประเทศไทยของสำนักงานพัฒนารัฐบาลดิจิตอล (องค์การมหาชน) (Digital Government Development Agency (Public Organization) (DGA) พบว่าประเทศไทย มีการพบภัยคุกคามในทุกรูปแบบ

ตารางที่ 2-1 สถิติภัยคุกคามทางไซเบอร์ ประจำปี 2562

| ประเภทภัยคุกคาม / เดือน | ม.ค. | ก.พ. | มี.ค. | เม.ย. | พ.ค. | มิ.ย. | ก.ค. | ส.ค. | ก.ย. | ต.ค. | พ.ย. | ธ.ค. | รวม |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Abusive content | 0 | 0 | 1 | 6 | 98 | 7 | 5 | 2 | 2 | 1 | 1 | 1 | **124** |
| Availability | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 21 | 29 | 8 | 17 | 4 | **79** |
| Fraud | 87 | 46 | 59 | 60 | 84 | 53 | 128 | 69 | 86 | 93 | 88 | 59 | **912** |
| Information gathering | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 40 | 4 | 3 | 10 | 3 | **60** |
| Information security | 39 | 0 | 0 | 3 | 40 | 1 | 45 | 22 | 11 | 0 | 1 | 3 | **165** |
| Intrusion Attempts | 78 | 90 | 62 | 33 | 24 | 43 | 84 | 22 | 9 | 4 | 11 | 7 | **467** |
| Intrusions | 12 | 10 | 24 | 13 | 34 | 12 | 6 | 46 | 39 | 9 | 5 | 8 | **218** |
| Malicious code | 20 | 8 | 13 | 7 | 6 | 7 | 16 | 88 | 51 | 46 | 84 | 90 | **436** |
| Other | 0 | 0 | 0 | 3 | 0 | 0 | 0 | 0 | 5 | 1 | 0 | 0 | **9** |
| **รวม** | **236** | **154** | **159** | **125** | **286** | **123** | **284** | **310** | **236** | **165** | **217** | **175** | **2470** |
| | | | | | | | | | | | | | |

ที่มา : https://dga.or.th/upload/download/file_769c60982e4c374dcd33b41c29227a31.pdf, 2562

3. ผู้คุกคามทางไซเบอร์

ผู้คุกคามทางไซเบอร์หรือกลุ่มบุคคลและ/หรือองค์กรที่มีความชำนาญในการปฏิบัติการ ภัยไซเบอร์ แบ่งออกเป็น 5 ประเภท (นงรัตน์ สายเพชร , 2556) ดังนี้

3.1 กลุ่มที่มีความประสงค์ร้าย

กลุ่มนี้เป็นกลุ่มที่ดำเนินการในระดับประเทศ ซึ่งอาจเป็นรัฐบาลที่มีความขัดแย้งมุ่งโจมตีในระดับกองทัพของประเทศฝ่ายตรงข้าม โดยมีวัตถุประสงค์สร้างความเสียหายให้เกิดกับประเทศกลุ่มเป้าหมาย ทั้งในรูปแบบของสงครามตามแบบ และสงครามไม่ตามแบบ หรืออาจเป็นเพียงแค่การก่อกวนเว็บไซต์ เปลี่ยนภาพหน้าจอของเว็บไซต์ ซึ่งเป็นการโจมตีที่ไม่ยาก แต่ทำให้เกิดความเสียหายต่อภาพลักษณ์ในระดับประเทศได้ การจารกรรมข้อมูลที่สำคัญ ซึ่งอาจส่งผลต่อเศรษฐกิจของประเทศคู่แข่ง รวมถึงการทำลายโครงสร้างพื้นฐานของระบบเทคโนโลยีสารสนเทศ

3.2 กลุ่มผู้ก่อการร้าย

กลุ่มผู้ก่อการร้ายนี้ มีความมุ่งหวังจะทำลายผลประโยชน์แห่งชาติของประเทศเป้าหมาย แต่ระดับความเสียหายอาจยังไม่สูงเท่ากลุ่มที่ทำสงครามในระดับประเทศ อาจด้วยเหตุผลด้านทรัพยากร เครื่องมืออุปกรณ์ที่ใช้งาน รวมถึงอาวุธยุทโธปกรณ์ในการทำลายล้างยังมีจำกัด

อย่างไรก็ตามแม้ประเทศที่ถูกโจมตีทางไซเบอร์จากกลุ่มก่อการร้ายนี้อาจมีความเสียหายที่ไม่มากนัก แต่ภาพลักษณ์ของประเทศอาจเสียหายค่อนข้างมาก กลุ่มผู้ก่อการร้ายเหล่านี้ยังนำไซเบอร์มาใช้ประโยชน์แต่ตน เช่น เป็นช่องทางการสื่อสารข้อมูลที่สะดวก รวดเร็ว และเจ้าหน้าที่รัฐก็ยังติดตามได้ยาก นอกจากนี้ใช้ไซเบอร์ในการเผยแพร่ความสำเร็จของตน เพื่อใช้การขอทุน และการเผยแพร่แนวความคิดที่เป็นภัย

3.3 สายลับภาคเอกชน / องค์กรอาชญากรรม

กลุ่มนี้เป็นกลุ่มระดับองค์กร ผลประโยชน์ที่กลุ่มต้องการเป็นเรื่องของทรัพย์สินมากกว่าเรื่องอื่น ๆ ดังนั้นการโจมตีจึงมีเป้าหมายเพื่อจารกรรมข้อมูลที่เชื่อมโยงไปทางด้านการเงิน ทั้งจากองค์กรภาครัฐ และภาคเอกชนต่าง ๆ ที่ต้องการนำข้อมูลสำคัญไปหารายได้ หรืออาจมีรัฐบาลต่างประเทศที่เป็นคู่ขัดแย้งสนับสนุนเพื่อการทำลายประเทศคู่แข่งในด้านเศรษฐกิจ

3.4 แฮกเกอร์

เป็นกลุ่มที่พยายามหาช่องโหว่ของระบบ ลักลอบเจาะระบบเข้าไปทำอันตราย หรือขโมยข้อมูลข่าวสารที่สำคัญ ก่อให้เกิดความเสียหายต่อเป้าหมาย การดำเนินการอาจทำเป็นกลุ่มหรือบุคคล อาจดำเนินการเพียงแค่การฝึก หรือประกาศความสามารถของตนโดยไม่หวังจะทำร้ายใครก็ได้ องค์กรหน่วยงานบางแห่งอาจดำเนินการจ้างเหล่าแฮกเกอร์นี้ ทั้งนี้ไม่ใช่เพื่อไปเจาะช่องโหว่ของคู่แข่งขัน แต่ให้เจาะระบบของหน่วยงานตนเองเพื่อดูช่องโหว่ของระบบ และดำเนินการแก้ไขต่อไป

3.5 แฮกทิวิส

กลุ่มแฮกเกอร์กลุ่มนี้ไม่ได้หวังประโยชน์ทางด้านการเงิน หรือสร้างชื่อเสียงให้กับตนเอง เหมือนกลุ่มแฮกเกอร์ทั่วไป แต่เป็นกลุ่มที่ทำงานทางด้านการเมือง ต้องการความเปลี่ยนแปลงทางการเมือง ดำเนินการโดยการนำเสนอความคิด สร้างเหตุการณ์ หาข้อมูลที่มาสนับสนุนต่าง ๆ ให้ส่งผลต่อการเมือง ไม่ได้ส่งผลต่อโครงสร้างพื้นฐานของระบบเทคโนโลยีสารสนเทศ หรือข้อมูลทางด้านการเงิน กลุ่มนี้อาจไม่ได้ดำเนินการตามความเชื่อของตนเอง แต่อาจได้รับการว่าจ้างให้ดำเนินการโฆษณาชวนเชื่อ ดัดแปลง เปลี่ยนแปลง หรือส่งเสริม โดยใช้หลักทางจิตวิทยา ให้กลุ่มคนมีความคิด ความเชื่อ และดำเนินการไปตามวัตถุประสงค์ที่ต้องการ

4. แนวคิดเกี่ยวกับการกลั่นแกล้งทางไซเบอร์ (Cyber Bullying)

การกลั่นแกล้งทางไซเบอร์ คือการรังแกและคุกคามผ่านสื่อสังคมออนไลน์ โดยใช้อุปกรณ์อิเล็กทรอนิกส์ผ่านระบบอินเทอร์เน็ต ซึ่งการแพร่ข้อความด้วยวิธีนี้สามารถกระทำได้ง่าย และกระจายอย่างรวดเร็ว จัดได้ว่าเป็นอาชญากรรมทางคอมพิวเตอร์ประเภทหนึ่ง การกลั่นแกล้งทางไซเบอร์เป็นการกระทำโดยเจตนาที่นำไปสู่ความเครียดทางอารมณ์ ทำให้ผู้ถูกกลั่นแกล้งเกิดความทุกข์ซ้ำ ๆ จากข้อความอิเล็กทรอนิกส์ดังกล่าว การกลั่นแกล้งทางไซเบอร์นี้ รวมถึงการคุกคามที่มีเนื้อหาเกี่ยวกับเรื่องเพศ ความรุนแรง การดูถูก ยังรวมถึงการส่งจดหมายอิเล็กทรอนิกส์ไปรบกวน ซึ่งก่อให้เกิดความหงุดหงิด รำคาญแก่ผู้ได้รับด้วย นอกจากนี้ยังมีพฤติกรรมความก้าวร้าวของบุคคลหรือกลุ่มบุคคลที่เจตนาใช้เครื่องมืออิเล็กทรอนิกส์ ทำร้ายเหยื่อที่ไม่สามารถปกป้องตนเองจากการกระทำนั้นได้ โดยปัจจุบันการกลั่นแกล้งทางไซเบอร์ดังกล่าวมีจำนวนสูงขึ้นมาก อาจสืบเนื่องมาจากอัตราการใช้งานอินเทอร์เน็ตที่เพิ่มสูงขึ้นทำให้ผู้คนเข้าถึงข้อมูลข่าวสารได้อย่างสะดวกและรวดเร็ว

ลักษณะของการกลั่นแกล้งทางไซเบอร์ มีลักษณะดังนี้

1. การข่มขู่ใส่ร้าย (Harassment) เป็นการกลั่นแกล้งโดยการส่งข้อความโจมตีในทางเสียหายด้วยความคึกคะนองไปยังบุคคลอื่น หรือกลุ่มคนและทำซ้ำเป็นประจำหลายครั้ง ทั้งนี้ การพูดคุยในโลกไซเบอร์ เป็นอีกรูปแบบหนึ่งของการใช้คำพูดที่ข่มขู่ ก้าวร้าว หยาบคาย นำไปสู่การทำร้ายร่างกายในโลกความเป็นจริง

2. การยั่วโมโห (Flaming) มีความคล้ายคลึงกับการข่มขู่ใส่ร้าย แต่จะมีการโต้ตอบกันทางอีเมล์ ข้อความโต้ตอบในแอพพลิเคชั่นแบบต่าง ๆ เป็นการกลั่นแกล้งประเภทหนึ่งที่เผยแพร่สู่สาธารณะโดยบ่อยครั้งมีการใช้ภาษาหรือภาพที่ส่อถึงบุคคลคนใดคนหนึ่งเป็นพิเศษ

3. การกีดกัน (Exclusion) การกีดกันเป็นการกระทำที่แยกบุคคลหนึ่งจากกลุ่มที่ออนไลน์ เช่น การสนทนาโดยส่งข้อความทันที การแชท ทั้งนี้ในกลุ่มจะมีการวิพากษ์ วิจารณ์ ในแง่ร้ายและข่มขู่จนกว่าบุคคลนั้นจะถอนตัวออกไป

4. การเผยแพร่ออกนอกกลุ่ม (Outing) การเผยแพร่ออกนอกกลุ่ม คือ การกลั่นแกล้งโดยแบ่งเอาข้อมูล ภาพ คลิปวีดีโอส่วนบุคคล หรือข้อมูลส่วนบุคคล ไปเผยแพร่สู่สาธารณะโดยบุคคลนั้นเป็นคนที่ออกจากกลุ่มไปแล้ว ผู้ที่ออกนอกกลุ่มไปแล้ว โดยจะรู้ว่าข้อมูลถูกเผยแพร่หลังจากที่ข้อมูลส่งต่อกันในอินเทอร์เน็ต

5. การแอบอ้าง (Masquerading) การแอบอ้างหรือเสแสร้งนั้นเป็นสถาการณ์การกลั่นแกล้งแบบหนึ่ง โดยสร้างเรื่องตลกที่มาจากลักษณะเฉพาะตัวที่เกี่ยวข้องกับบุคคลที่ถูกขมขู่ โดยปิดบังชื่อ นอกจากสร้างเรื่องตลก ยังมีการกลั่นแกล้งโดยปลอมเป็นบุคคลอื่น เพื่อส่งข้อความประสงค์ร้ายต่อเหยื่อด้วย

## นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.2562-2565)

### การป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

เสริมสร้างความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดเป้าหมายเชิงยุทธศาสตร์ ตัวชี้วัด และกลยุทธ์ ดังนี้

1. เป้าหมายเชิงยุทธศาสตร์ ประเทศไทยมีความมั่นคงปลอดภัยและมีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์

2. ตัวชี้วัด

2.1 ระดับความพร้อมของไทยในการป้องกันความเสี่ยงจากการโจมตี ด้านไซเบอร์ที่สอดคล้องกับหลักสากล

2.2 ระบบป้องกันทางไซเบอร์ที่มีประสิทธิภาพ สามารถปกป้องข้อมูลอิเล็กทรอนิกส์ของรัฐบาล ตลอดจนโครงสร้างพื้นฐานสำคัญด้านไซเบอร์

3. กลยุทธ์

3.1 พัฒนาขีดความสามารถ ทั้งองค์กรภาครัฐ ฝ่ายทหาร พลเรือน และตำรวจและภาคส่วนต่าง ๆ ภายในประเทศ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ ตลอดจนรองรับสังคม ดิจิทอล

3.2 พัฒนากรอบความร่วมมือระหว่างประเทศ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

3.3 พัฒนาทรัพยากรมนุษย์ องค์ความรู้ และความตระหนักรู้ถึงความสำคัญของภัยคุกคามความมั่นคงทางไซเบอร์

3.4 ป้องกันภัยคุกคามด้านไซเบอร์ และกำจัดความเสี่ยงที่อาจนำไปสู่สงครามไซเบอร์ เพื่อเสริมสร้างความปลอดภัยทางไซเบอร์ โดยบูรณาการการจัดการความมั่นคงทางไซเบอร์ระหว่างหน่วยงานภาครัฐ ตลอดจนเสริมสร้างเครือข่ายความร่วมมือกับทุกภาคส่วน ทั้งภายในและภายนอกประเทศ

3.5 พัฒนาการบังคับใช้กฎหมาย ระเบียบต่าง ๆ เพื่อความมั่นคงปลอดภัยไซเบอร์ รวมถึงพัฒนาเทคโนโลยีสำหรับงานสืบสวนและป้องกันอาชญากรรมไซเบอร์

3.6 ส่งเสริมการพัฒนาขีดความสามารถขององค์กรทุกภาคส่วน/บุคลากรที่เกี่ยวข้องให้มีความรู้ความชำนาญด้านไซเบอร์อย่างต่อเนื่อง

## ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ.2560-2564)

### วัตถุประสงค์

1. เพื่อสร้างความเชื่อมั่น ความไว้วางใจในทุกภาคส่วนต่อการดำเนินกิจการทางไซเบอร์ทุกรูปแบบ

2. เพื่อปกป้องโครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศ และพัฒนาด้านศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

3. เพื่อปกป้องผลประโยชน์ และความมั่นคงของชาติภัยคุกคามรูปแบบเดิมและภัยคุกคามรูปแบบใหม่

4. เพื่อเสริมสร้างเศรษฐกิจดิจิทัล

5. เพื่อบูรณาการและประสานความร่วมมือรวมทั้งการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัยไซเบอร์

6. เพื่อพัฒนาศักยภาพของหน่วยงาน และเพิ่มขีดความสามารถของบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

7. เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซอย่างมีความรับผิดชอบ

8. เพื่อส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

9. เพื่อส่งเสริมบทบาทของไทยในการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งในระดับประเทศ ระดับภูมิภาคอาเซียนและระดับนานาชาติ

### เป้าหมาย

1. ภาคส่วนต่าง ๆ เชื่อมั่นและไว้วางใจในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

2. โครงสร้างพื้นฐานสำคัญที่บริหารจัดการด้วยระบบสารสนเทศและประเทศโดยรวมมีขีดความสามารถในการรับมือกับภัยคุกคามทางไซเบอร์

3. ผลประโยชน์และความมั่นคงของชาติได้รับการปกป้องจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

4. ประเทศเปลี่ยนผ่านสู่เศรษฐกิจที่ใช้เทคโนโลยีดิจิทัลได้อย่างราบรื่นและยั่งยืน

5. ทุกภาคส่วนมีความตระหนักถึงภัยคุกคามทางไซเบอร์ และร่วมมือกันด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

6. ประเทศไทยมีวัฒนธรรมการใช้ไซเบอร์สเปซอย่างมีความรับผิดชอบ

7. การบูรณาการและการประสานความร่วมมือ รวมทั้งการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

8. งานด้านการป้องกันและปราบปรามอาชญากรรมมีความเข้มแข็ง การสืบสวนและงานข่าวมีคุณภาพและมั่นคงปลอดภัย

9. หน่วยงานมีความพร้อมสามารถตอบสนองการปฏิบัติการได้อย่างถูกต้องและรวดเร็ว

10. บุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์ มีความเชี่ยวชาญและมีศักยภาพในการปฏิบัติงาน

11. ไทยมีบทบาทในการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ ในระดับนานาชาติและลดความขัดแย้งทางไซเบอร์ระหว่างรัฐ

**ประเด็นยุทธศาสตร์**

ประเด็นยุทธศาสตร์ที่ 1 เสริมสร้างความเชื่อมั่นและความไว้วางใจในทุกภาคส่วนในการดำเนินกิจกรรมทางไซเบอร์ทุกรูปแบบ

ประเด็นยุทธศาสตร์ที่ 2 ปกป้องโครงสร้างพื้นฐานสำคัญ ที่บริหารจัดการด้วยระบบสารสนเทศและพัฒนาศักยภาพด้านการรับมือภัยคุกคามทางไซเบอร์

ประเด็นยุทธศาสตร์ที่ 3 ปกป้องผลประโยชน์และความมั่นคงของชาติ ให้รอดพ้นจากภัยคุกคามรูปแบบเดิมและรูปแบบใหม่

ประเด็นยุทธศาสตร์ที่ 4 เสริมสร้างระบบเศรษฐกิจดิจิทัล

ประเด็นยุทธศาสตร์ที่ 5 สร้างความตระหนักและส่งเสริมความร่วมมือภายในประเทศด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

ประเด็นยุทธศาสตร์ที่ 6 เพื่อส่งเสริมวัฒนธรรมการใช้ไซเบอร์สเปซในทางที่เหมาะสม

ประเด็นยุทธศาสตร์ที่ 7 ส่งเสริมงานด้านการป้องกันและปราบปรามอาชญากรรม

ประเด็นยุทธศาสตร์ที่ 8 ส่งเสริมบทบาทที่สร้างสรรค์ของไทย ในความร่วมมือเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภูมิภาคและระดับนานาชาติ

**ปัจจัยแห่งความสำเร็จ**

1. รัฐบาลให้ความสำคัญกับการรักษาความปลอดภัยไซเบอร์แห่งชาติ และผลักดันให้เกิดผลเป็นรูปธรรมอย่างจริงจัง

2. หน่วยงานต่างๆ ได้นำแนวทางตามยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติไปปฏิบัติ และจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานตัวเอง และปฏิบัติตามแผนฯ อย่างจริงจัง

3. ทุกภาคส่วนที่เกี่ยวข้อง ทั้งภาครัฐ เอกชน และภาคประชาชน ให้ความร่วมมือและมีส่วนร่วมในการสร้างความตระหนักรู้เรื่องการรักษาความปลอดภัยไซเบอร์

4. จัดให้มีการทบทวนประเมินผลการดำเนินการตามยุทธศาสตร์ทุก 2 ปี

## การพัฒนาบุคลากรของกองทัพบกในการรับมือกับภัยคุกคามทางไซเบอร์

การพัฒนาบุคลากรของกองทัพบกในการรับมือกับภัยคุกคามทางไซเบอร์นั้น ควรต้องมีการกำหนดหน้าที่ และขอบเขตของงานให้กับกำลังพลที่ต้องรับผิดชอบ เมื่อทราบขอบเขตของงานแล้ว กองทัพบกดำเนินการจัดหาบุคลากรที่มีความรู้ความสามารถมาบรรจุเพื่อให้สามารถปฏิบัติงานได้ หรือส่งเสริมการศึกษาอบรมเพิ่มเติม เพื่อให้กำลังพลที่มีอยู่สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ สำหรับบุคลากรที่จะดำเนินการในการรับมือกับภัยคุกคามทางไซเบอร์ สามารถกำหนดได้เป็น 3 ระดับ คือ

1. ระดับผู้บริหาร/ผู้วางแผน
2. ระดับเทคนิค
3. ระดับปฏิบัติการ

โดยแต่ระดับมีการกำหนดวัตถุประสงค์ ขอบเขตและหน้าที่ความรับผิดชอบ ให้ชัดเจน แต่อย่างไรก็ตามระดับที่สูงกว่าต้องมีความรู้ความสามารถในการปฏิบัติหน้าที่แทนระดับที่ต่ำกว่าได้ ในขณะเดียวกัน ระดับที่ต่ำกว่าสามารถที่จะให้ข้อมูล ข้อเสนอแนะ แนวทางการปฏิบัติ การแก้ไขปัญหา ให้ระดับที่สูงกว่า เพื่อนำไปวางแผน ตัดสินใจ ดำเนินการได้อย่างเหมาะสมในแต่ละสถานการณ์

1. ระดับผู้บริหาร/ผู้วางแผนด้านการรักษาความปลอดภัยทางไซเบอร์ต้องพัฒนาให้มีขีดความสามารถในการดำเนินการดังต่อไปนี้

1.1 กำหนดนโยบายการรักษาความปลอดภัยได้ (Network Security Policy) โดยมีความรู้ด้านเทคโนโลยีสารสนเทศ และมีความรู้ความเข้าใจในขีดความสามารถขององค์กร เพื่อเป็นแนวทางและสนับสนุนการรักษาความปลอดภัย

1.2 จัดโครงสร้างระบบรักษาความปลอดภัยขององค์กร เพื่อสามารถบริหารจัดการควบคุมกำกับดูแลการนำนโยบายการรักษาความปลอดภัยไปใช้ให้มีประสิทธิภาพ

1.3 กำหนดแผนบริหารความเสี่ยง (Risk Management) โดยมีความรู้ความเข้าใจในจุดอ่อนและภัยคุกคามขององค์กร รวมถึงเหตุการณ์ที่ไม่ปกติและภัยพิบัติทางธรรมชาติ

1.4 ควบคุมกำกับดูแลเมื่อเกิดเหตุการณ์ผิดปกติ ตามแผนบริหารความเสี่ยงที่กำหนดไว้ โดยสามารถรายงานเหตุการณ์ จุดอ่อน ช่องโหว่ที่เกี่ยวข้องกับความปลอดภัยให้ผู้บังคับบัญชาทราบ และบริหารจัดการเหตุการณ์ละเมิดความปลอดภัยได้อย่างรวดเร็วและมีประสิทธิภาพ เพื่อไม่ให้เกิดความสูญเสีย หรือสูญเสีย เสียหายให้น้อยที่สุด

1.5 ทบทวนนโยบายการรักษาความปลอดภัยทบทวนแผนบริหารความเสี่ยงหรืออื่น ๆ ตามความเหมาะสม

1.6 วางแผนการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศอย่างเหมาะสมเพียงพอ ได้แก่

1.6.1 การจัดการทรัพย์สินให้เพียงพอต่อการปฏิบัติงาน กำหนดการเข้าถึงทรัพยากร และข้อมูลที่มีชั้นความลับ

1.6.2 การรักษาความปลอดภัยในระดับบุคลากร มีจุดประสงค์เพื่อลดความเสี่ยงที่อาจเกิดขึ้นกับความผิดพลาดของคน การขโมย การหลอกลวง หรือการใช้งานระบบในทางที่ผิด

1.6.3 การรักษาความปลอดภัยด้านกายภาพและสภาพแวดล้อม มีจุดมุ่งหมายเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตที่จะเข้าไปทำลาย ขโมย ใช้ทรัพยากร หรือขัดขวางการปฏิบัติหน้าที่

1.7 ป้องกันการขัดต่อกฎหมายเกี่ยวกับพระราชบัญญัติคอมพิวเตอร์ และกฎหมายแพ่ง กฎหมายอาญา กฎหมายอื่น ๆ รวมถึง กฎ ระเบียบข้อบังคับ และสัญญาต่าง ๆ

2. ระดับเทคนิค การพัฒนาบุคลากรในระดับนี้ค่อนข้างยาก เนื่องจากต้องใช้บุคลากรที่มีความเชี่ยวชาญพิเศษโดยเฉพาะ และเนื่องจากเทคโนโลยีสารสนเทศ เป็นเทคโนโลยีที่พัฒนา และเปลี่ยนแปลงอย่างรวดเร็ว บุคลากรในระดับเทคนิค จึงต้องมีการฝึกอบรมอย่างสม่ำเสมอและต่อเนื่องเพื่อให้ทันกับโลกที่เปลี่ยนแปลงอย่างรวดเร็ว โดยกำลังพลที่ปฏิบัติหน้าที่ในระดับเทคนิค ควรพัฒนาให้มีความรู้ความสามารถในเรื่องดังต่อไปนี้

2.1 การเฝ้าระวังการใช้งานของระบบซึ่งเป็นกลไกใช้สำหรับการตรวจสอบการปฏิบัติตามนโยบายการใช้งานของกำลังพล รวมถึงแอพลิเคชันที่ใช้งานว่ามีความผิดปกติหรือไม่อย่างไร

2.2 การปฏิบัติตามนโยบาย เป็นการตรวจสอบว่ามีการฝ่าฝืนนโยบายหรือระเบียบในด้านการรักษาความปลอดภัยหรือไม่ ซึ่งอาจใช้ซอฟแวร์ที่สามารถตรวจสอบได้อัตโนมัติ รวมถึงต้องตรวจสอบล็อกไฟล์ หรือทำการสุ่มเลือกบางระบบเพื่อทำการสแกน

2.3 ระบบพิสูจน์ทราบตัวตน กำหนดกลไกในการตรวจสอบการเข้าสถานที่ที่ต้องห้าม พิสูจน์ทราบอาจโดยการใช้รหัสผ่าน สมาร์ทการ์ด หรือไบโอเมติก เป็นต้น รวมถึงแก้ปัญหาหากระบบพิสูจน์ทำงานขัดข้อง

2.4 รักษาความปลอดภัยในการใช้งานอินเทอร์เน็ต เช่น ติดตั้งไฟร์วอลล์ (Firewall) เพื่อควบคุมการเข้าถึง หรือ VPN (Virtual Private Network) เพื่อเปลี่ยนโครงสร้างของเครือข่ายอินเทอร์เน็ตให้เปรียบเสมือนเครือข่ายภายใน

2.5 ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection System) เป็นระบบเตือนภัยของเครือข่าย มีสัญญาณเตือนเมื่อมีเหตุการณ์ผิดปกติ

2.6 การเข้ารหัสข้อมูล (Encryption) เป็นวิธีการปกป้องความลับ (Confidentiality) ของข้อมูล การเข้ารหัสข้อมูลมี 2 รูปแบบ คือ เข้ารหัสเพื่อไม่ให้ผู้อื่นเข้าไปอ่านข้อมูลได้ และเข้ารหัสเพื่อตรวจสอบว่ามีผู้เข้าไปทำการเปลี่ยนแปลงแก้ไขข้อมูล

2.7 การรักษาความปลอดภัยทางกายภาพ บางครั้งอาจถูกแยกออกไปจากการรักษาความปลอดภัยข้อมูล หรือด้านการสื่อสาร แต่อย่างไรก็ตามการรักษาความปลอดภัยทางกายภาพก็สามารถทำงานร่วมกับเจ้าหน้าที่ฝ่ายเทคนิคในการช่วยอุดช่องโหว่หรือจุดอ่อนของระบบได้ โดยนำเทคโนโลยีที่เหมาะสมมาใช้ เช่น กล้องวงจรปิด คีย์การ์ด ระบบไบโอเมตริก รหัสผ่าน เป็นต้น

ซึ่งระเบียบปฏิบัติที่ถูกต้องรวมถึงขั้นตอนที่เหมาะสม หรือวิธีพิสูจน์ทราบที่แน่ชัด เป็นการป้องกันไม่ให้ผู้ไม่ประสงค์ดีสามารถบุกรุกเข้าโดยง่าย

2.8 การตรวจสอบ (Audit) เป็นกระบวนการตรวจสอบ ประเมินสถานการณ์ การรักษาความปลอดภัยขององค์กร เพื่ออาจนำไปกำหนดนโยบาย ระเบียบปฏิบัติ หรือติดตั้งระบบรักษาความปลอดภัยใหม่ ๆ ที่จำเป็น ซึ่งการตรวจสอบจะมี 3 ประเภทดังนี้

2.8.1 การตรวจสอบการปฏิบัติตามนโยบายเป็นการตรวจสอบว่ามีการปฏิบัติตามระดับความรักษาความปลอดภัยที่ได้คาดหวังไว้หรือไม่ โดยเจ้าหน้าที่เทคนิคอาจดำเนินการเองหรือให้บุคลากรจากภายนอกเข้ามาช่วยตรวจสอบ

2.8.2 การประเมินโครงการใหม่เนื่องจากคอมพิวเตอร์ และเครือข่ายเป็นเทคโนโลยีที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา จุดอ่อนหรือช่องโหว่เก่าอาจถูกป้องกันไว้หมดแล้ว แต่เทคโนโลยีใหม่อาจมีช่องโหว่ หรือจุดอ่อนใหม่ที่ยังไม่ได้ค้นพบ ดังนั้นหากมีการติดตั้งหรือพัฒนาระบบใหม่ควรมีการตรวจสอบหรือทดลองระบบใหม่ก่อนทุกครั้ง ว่ามีความปลอดภัยมากน้อยเพียงใดก่อนที่จะนำไปใช้งาน

2.8.3 การทดลองเจาะระบบ (Penetration Testing) เป็นการใช้เครื่องมือเพื่อทดลองเจาะระบบ จากจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักทั่วไป หากเจาะระบบสำเร็จ ข้อมูลที่ได้คือทราบว่าองค์กรมีจุดอ่อนหรือช่องโหว่อย่างไร

2.9 การฝึกอบรม เจ้าหน้าที่เทคนิคนอกจากต้องเข้ารับการฝึกอบรมอย่างสม่ำเสมอแล้ว ยังต้องออกแบบและทำการฝึกอบรมให้ทั้งกับเจ้าหน้าที่ที่ปฏิบัติงานด้านรักษาความปลอดภัย รวมถึงพนักงานทั่วไป อาจมีการเชิญวิทยากร หรือผู้เชี่ยวชาญภายนอกมาฝึกอบรม นำเสนอข้อมูลเกี่ยวกับเทคนิค หรือเทคโนโลยีใหม่ๆ

3. ระดับปฏิบัติงาน เป็นบุคลากรที่รับผิดชอบเกี่ยวกับการรักษาความปลอดภัยทั่วไป ซึ่งต้องมีความรู้ความเข้าใจ ทราบว่าการรักษาความปลอดภัยมีความสำคัญอย่างไร รับรู้ว่าข้อมูลใดมีความสำคัญและความลับขององค์กร รู้วิธีจัดการกับรหัสผ่าน และช่วยป้องกันการโจมตีวิศวกรรมสังคม (Social Engineering) และสามารถสังเกตความผิดปกติ และรายงานให้ผู้บังคับบัญชาตามลำดับชั้นทราบ

## มาตรฐานการรักษาความปลอดภัยทางไซเบอร์ในระดับสากล

### 1. มาตรฐาน ISO/IEC17799:2005 (Second Edition) หรือ BS77991

มาตรฐาน ISO/IEC17799: 2005 (Second Editon) ถูกประกาศใช้อย่างเป็นทางการเมื่อเดือนมิถุนายน ปี 2005 มีการปรับปรุงแก้ไขมาจากต้นฉบับ ISO/ IEC17799: 2000 (First Edition) จากปี 2000 โดยได้กำหนดมาตรฐานการรักษาความปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์เป็น 3 ระดับ คือ ระดับ 1 ควรปฏิบัติ 31 ข้อ ระดับ 2 ควรปฏิบัติ 104 ข้อ และระดับ 3 ซึ่งเป็นระดับความปลอดภัยสูงสุด ควรปฏิบัติทั้งหมด 144 ข้อ

**2. มาตรฐาน Cobit (Control Objective for Information and Related Technogy)**

มาตรฐาน CobiT พัฒนาโดย ISACA (http://www.isaca.org) และ IT Governane Institute (http://itgi.org) เพื่อองค์กรที่ต้องการมุ่งสู่การเป็น “ไอทีภิบาล” หรือ “IT Governance” มาตรฐาน CobiT เป็นแนวคิดและแนวทางปฏิบัติของผู้บริหารระบบสารสนเทศ และเป็นแนวทางปฏิบัติสำหรับผู้ตรวจสอบระบบสารสนเทศ

**3. CompTIA Security+**

คือประกาศนียบัตรการรับรองความรู้ด้านความปลอดภัย สำหรับผู้เชี่ยวชาญด้านไอที ซึ่งมีเนื้อหาอ้างอิงจากความรู้เบื้องต้นที่จำเป็นสำหรับการรักษาความปลอดภัยทางไซเบอร์ และเป็นจุดเริ่มต้นทางด้านความคิดที่ใช้สำหรับงานด้านความปลอดภัยในระดับกลาง - ระดับสูง โดย CompTIA Security+ ได้รับการรับรองมาตรฐานโดย ANSI และยังสอดคล้องกับมาตรฐาน ISO 17024 ซึ่งเป็นการยืนยันถึงมาตรฐาน และการปรับปรุงคุณภาพอย่างต่อเนื่อง โดยหัวข้อต่าง ๆ ในวัตถุประสงค์การเรียนรู้ของ CompTIA Security+ เป็นผลลัพท์จากการวิจัยและพัฒนาโดยผู้เชี่ยวชาญด้าน Information Security ในทุกมิติเพื่อให้สอดคล้องกับความต้องการขององค์กรต่าง ๆ อย่างแท้จริง

## หลักสูตรนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมจอมเกล้า ประจำปี 2562

1. ชื่อหลักสูตร : หลักสูตรโรงเรียนนายร้อยพระจุลจอมเกล้า พ.ศ.2562 (5ปี) ประกอบด้วย
   1.1 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล
   Bachelor of Engineering Program in Mechanical Engineering
   1.2 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร
   Bachelor of Engineering Program in Electrical Engineering (Communication Engineering)
   1.3 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ
   Bachelor of Engineering Program in Industrial Engineering
   1.4 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา
   Bachelor of Engineering Program in Civil Engineering
   1.5 หลักสูตรวิศวกรรมบัณฑิต สาขาวิชาวิศวกรรมแผนที่
   Bachelor of Engineering Program in Surveying and Mapping
   1.6 หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์
   Bachelor of Science Program in Computer Science
   1.7 หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี
   Bachelor of Science Program in Science and Technology
   1.8 หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา
   Bachelor of Arts Program in Social Science for Development

2. หน่วยงานที่รับผิดชอบ : โรงเรียนนายร้อยพระจุลจอมเกล้า โดยหน่วยงานที่จัดการฝึกศึกษา อบรมได้แก่

2.1 ส่วนการศึกษา โรงเรียนนายร้อยพระจุลจอมเกล้า

2.2 ส่วนวิชาทหาร โรงเรียนนายร้อยพระจุลจอมเกล้า

2.3 กรมนักเรียนนายร้อยรักษาพระองค์ โรงเรียนนายร้อยพระจุลจอมเกล้า

3. ปีการศึกษาที่เริ่มใช้หลักสูตร : ปีการศึกษา 2558

4. วัตถุประสงค์ของหลักสูตร : ผลิตนายทหารสัญญาบัตรให้เป็นนายทหารหลักของกองทัพบก ที่พร้อมด้วยคุณลักษณะดังนี้

4.1 เป็นแบบฉบับของนายทหารสัญญาบัตร ผู้มีลักษณะผู้นำดี มีวินัย รู้แบบธรรมเนียมของกองทัพ อุทิศตนเพื่อชาติและประชาชน

4.2 มีความรู้ความสามารถพื้นฐานในการปฏิบัติการทางทหาร ในหมวดของหน่วยรบ รู้บทบาทต่าง ๆ รู้พื้นฐานการปฏิบัติการร่วมกับเหล่าทัพอื่น และมีพื้นฐานเพียงพอในการช่วยพัฒนาท้องถิ่นและประเทศชาติ

4.3 มีความมุ่งมั่นในการพัฒนาวิชาชีพทหารและช่วยพัฒนากองทัพ

4.4 มีความเข้มแข็งทั้งร่างกายและจิตใจเป็นสุภาพบุรุษ มีคุณธรรม สามารถพัฒนาและดำรงความเข้มแข็งของสมรรถภาพร่างกายทั้งในตนเองและเสริมสร้างให้แก่กำลังพลในหน่วยของตนได้

4.5 มีพื้นฐานความรู้วิทยาการระดับอุดมศึกษาพอ สำหรับเสริมสร้างคุณลักษณะข้างต้น เป็นผู้ที่ก้าวทันโลกทันเหตุการณ์ และผู้เรียนสาขาวิศวกรรมสามารถประกอบวิชาชีพวิศวกรรมได้

4.6 มีความสามารถในการฝึก สอน อบรมนายสิบและพลทหาร

5. ปรัชญาการศึกษาของโรงเรียนนายร้อยพระจุลจอมเกล้า

โรงเรียนนายร้อยพระจุลจอมเกล้าให้การศึกษาอบรม และดำเนินการฝึกนักเรียนนายร้อย เพื่อให้ผู้สำเร็จการศึกษามีคุณลักษณะอันจำเป็น และเพียงพอแก่การเป็นนายทหารประจำการในกองทัพบก เป็นแบบฉบับในด้านลักษณะผู้นำ มีสติปัญญารอบรู้ มีพื้นฐานและสามารถเพิ่มพูนความชำนาญในวิชาชีพทหาร มีจริยธรรมและความมุ่งมั่นในการอุทิศตนเพื่อรับใช้ชาติและประชาชน

นอกจากจะให้การศึกษาเพื่อมุ่งไปสู่ความมีสติปัญญารอบรู้เช่นเดียวกับการศึกษาระดับอุดมศึกษาแล้ว โรงเรียนนายร้อยพระจุลจอมเกล้ายังจะต้องฝึกและอบรมนักเรียนนายร้อยเพื่อเป็นนายทหารสัญญาบัตรที่มีบทบาทที่สำคัญยิ่งต่อกองทัพบกและประเทศชาติในอนาคต ดังนั้นการศึกษาในโรงเรียนนายร้อยพระจุลจอมเกล้า จะไม่เพ่งเล็งในด้านหลักสูตรหรือความรู้เฉพาะวิชาเพียงอย่างเดียวคำว่า “ศึกษา” จึงหมายถึง “คุณสมบัติและคุณลักษณะทั้งหมด ไม่ว่าทางด้านร่างกาย สมอง หรือจิตใจผู้ศึกษา ได้รับจากการเรียนรู้ การฝึกสอนหรืออบรม

การเรียนรู้ การฝึกสอนและอบรม มุ่งหมายให้ นักเรียนนายร้อยมีคุณสมบัติและคุณลักษณะอันเป็นสมุฏฐาน 4 ประการ คือ

1. รู้จักคิด รู้จักใช้เหตุผล

2. อุปนิสัย มีอุดมคติในเกียรติ ความซื่อสัตย์ วินัยและการเป็นผู้นำทางทหาร

3. มีรากฐานความรู้ในวิชาการต่าง ๆ อย่างแน่นแฟ้น สามารถนำไปใช้ในทางปฏิบัติได้อย่างถูกต้อง

4. รู้ถึงความสำคัญทางวิทยาการสาขาวิชาต่าง ๆ ที่ใช้ประโยชน์ในการทำสงคราม

6. เป้าหมายของการศึกษา

หลักสูตรการศึกษาของโรงเรียนนายร้อยพระจุลจอมเกล้า กำหนดไว้เพื่อให้ผู้สำเร็จการศึกษาบรรลุถึงคุณลักษณะดังต่อไปนี้

6.1 เพื่อให้นักเรียนนายร้อย ที่สำเร็จการศึกษาจากโรงเรียนนายร้อยพระจุลจอมเกล้า มีความรู้วิชาทหารสามารถเป็นผู้นำหน่วยทหารระดับหมวดปฏิบัติการรบได้อย่างมีประสิทธิภาพ มีความรู้พื้นฐานของเหล่าที่เลือกรับราชการอย่างกว้าง ๆ ที่จำเป็นต่อการรับราชการในช่วงแรก และมีพื้นฐานในการศึกษาต่อเพิ่มเติมจากโรงเรียนเหล่าสายวิทยาการ

6.2 มีพื้นฐานความรู้และความชำนาญในด้านจิตวิทยา และการเป็นผู้นำทหารอย่างเพียงพอที่จะนำไปปฏิบัติหน้าที่บังคับบัญชาทหาร

6.3 มีร่างกายสมบูรณ์แข็งแรง คล่องแคล่ว ว่องไว มีน้ำใจเป็นนักกีฬา รู้จักการเป็นผู้แพ้และเป็นผู้ชนะ โดยให้มีการฝึกพลศึกษาและเล่นกีฬาต่าง ๆ ตลอดเวลา 5 ปี

6.4 มีความรู้พื้นฐานเพียงพอทั้งทางวิทยาศาสตร์ วิศวกรรมศาสตร์ สังคมศาสตร์ มนุษย์ศาสตร์ และภาษาในระดับอุดมศึกษา

7. จำนวนนักเรียนนายร้อย เป็นไปตามนโยบายของกองทัพบก โดยประมาณดังนี้

ตารางที่ 2-2 จำนวนนักเรียนนายร้อยประจำปี 2562

| **ชั้นปี** | **2558** | **2559** | **2560** | **2561** | **2562** |
|---|---|---|---|---|---|
| 1 | 220 | 220 | 220 | 220 | 220 |
| 2 | | 220 | 220 | 220 | 220 |
| 3 | | | 220 | 220 | 220 |
| 4 | | | | 220 | 220 |
| 5 | | | | | 220 |

ที่มา : http://www.crma.ac.th/edu/EDU.pdf, 2562

## พันธกิจโรงเรียนนายร้อยพระจุลจอมเกล้าในการผลิตนายทหารสัญญาบัตร

พันธกิจของโรงเรียนนายร้อยพระจุลจอมเกล้าในการผลิตนายทหารสัญญาบัตร กำหนดไว้ดังนี้

1. ผลิตนักเรียนนายร้อยให้เป็นนายทหารสัญญาบัตรหลัก ตรงตามคุณลักษณะที่กองทัพบกต้องการ
2. เทิดทูนและดำรงไว้ซึ่ง สถาบันชาติ ศาสนา และพระมหากษัตริย์
3. ทำนุบำรุงศิลปวัฒนธรรม และขนบธรรมเนียมประเพณีทางทหาร
4. สร้างองค์ความรู้ทางวิชาการ วิชาทหาร การวิจัย และการเสริมสร้างคุณลักษณะผู้นำทางทหาร
5. ให้บริการทางวิชาการและวิชาชีพแก่สังคม
6. บริการจัดการโดยยึดหลักธรรมาภิบาล

## การพัฒนาหลักสูตรการรักษาความปลอดภัยทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า

ความเกี่ยวข้องกับพันธกิจของโรงเรียนนายร้อยพระจุลจอมเกล้า ตามประกาศนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.2562 - 2565) ในเรื่องการป้องกันและแก้ไขปัญหาทางไซเบอร์ โดยมีเป้าหมายทางยุทธศาสตร์ คือประเทศไทยมีความมั่นคงปลอดภัยและมีความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ มีกลยุทธ์ในการเพิ่มขีดความสามารถทั้งองค์กรภาครัฐ ฝ่ายทหาร พลเรือน และตำรวจ รวมทั้งภาคส่วนต่าง ๆ ภายในประเทศ เพื่อป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์ โดยใช้การพัฒนาทรัพยากรมนุษย์ องค์ความรู้ และตระหนักรู้ถึงความสำคัญของภัยคุกคามความมั่นคงทางไซเบอร์ การจัดทำหลักสูตรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ จึงควรจัดให้สอดคล้องกับนโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.2562 - 2565) รวมถึงสอดคล้องกับยุทธศาสตร์ทหารและแผนพัฒนากองทัพบก (พ.ศ. 2560 – 2564) ในเรื่องการมีขีดความสามารถในการปฏิบัติการสารสนเทศ และการปฏิบัติการในมิติไซเบอร์ และพันธกิจของโรงเรียนนายร้อยพระจุลจอมเกล้า รวมถึงเป็นไปตามแนวทางการพัฒนาบุคลากรของกองทัพบกในการรับมือกับภัยคุกคามทางไซเบอร์ในข้างต้น

### วัตถุประสงค์หลักสูตรการรักษาความปลอดภัยทางไซเบอร์

เพื่อผลิตนายทหารสัญญาบัตรให้เป็นนายทหารสัญญาบัตรหลักของกองทัพบกที่พร้อมด้วยคุณลักษณะดังนี้

1. มีความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ระดับปริญญาตรี
2. มีความรู้ความสามารถในการจัดการระบบความมั่นคงไซเบอร์ เพื่อให้สามารถปฏิบัติงานได้อย่างมีประสิทธิภาพและสามารถถ่ายทอดให้ผู้อื่นได้
3. มีความสามาถนำความรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ มาประยุกต์ใช้กับหน่วยงานกองทัพบกได้

4. มีความรู้ในด้านวิชาทหาร สามารถเป็นผู้บังคับหน่วย และนำหน่วยทหารระดับหมวดปฏิบัติการรบได้อย่างมีประสิทธิภาพ รวมทั้งมีความรู้พื้นฐานของเหล่าทั้งทางเทคนิคและยุทธวิธี

**แผนการพัฒนาปรับปรุงหลักสูตร**

1. ปรับปรุงหลักสูตรความมั่นคงปลอดภัยทางไซเบอร์ให้มีมาตรฐานการได้รับการรับรองโดยพัฒนาจากหลักสูตรในระดับสากล

2. ปรับปรุงหลักสูตรให้สอดคล้องกับความต้องการของกองทัพ และการเปลี่ยนแปลงของเทคโนโลยี

3. พัฒนาบุคลากรด้านการเรียนการสอนและบริการวิชาการให้มีประสบการณ์จากการนำความรู้ความมั่นคงปลอดภัยทางไซเบอร์ไปปฏิบัติงานจริง

**แผนการศึกษา**

โรงเรียนนายร้อยพระจุลจอมเกล้า โดยกองการศึกษา ได้มีการจัดทำแผนการศึกษาหลักสูตรวิทยาศาสตรบัณฑิตสาขาการรักษาความมั่นคงปลอดภัยทางไซเบอร์ แทนหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ โดยเริ่มดำเนินการมาในปี 2562 ดังนี้

1. กลุ่มวิชา/รายวิชาที่เปิดสอนโดยกองวิชาอื่น เพื่อให้สัมพันธ์กับหลักสูตรอื่นที่เปิดสอนในโรงเรียนนายร้อยพระจุลจอมเกล้า ดังนี้

1.1 กลุ่มวิชาสังคมศาสตร์

1.2 กลุ่มวิชามนุษยศาสตร์

1.3 กลุ่มวิชาภาษาศาสตร์

1.4 กลุ่มวิชาวิทยาศาสตร์บูรณาการ

1.5 กลุ่มวิชาพลศึกษา

1.6 กลุ่มวิชาเสริมสร้างลักษณะผู้นำ

1.7 กลุ่มวิชาทหาร

1.8 กลุ่มวิชาการฝึกภาคสนาม

1.9 กลุ่มวิชาวิทยาศาสตร์

2. กลุ่มวิชาความมั่นคงปลอดภัยทางไซเบอร์ ควรมีการปรับปรุงพัฒนาให้มีความรู้ความเข้าใจในเรื่องดังต่อไปนี้

2.1 พื้นฐานความมั่นคงปลอดภัยทางไซเบอร์

2.2 การบริหารจัดการระบบเทคโนโลยีสารสนเทศ

2.3 เทคโนโลยีและเครื่องมือที่เกี่ยวข้องกับการจัดการเครือข่าย

2.4 การรักษาความปลอดภัยครือข่าย

2.5 การรักษาความปลอดภัยของอุปกรณ์ฮาร์ดแวร์ ซอฟแวร์ ข้อมูล และสภาพแวดล้อม

2.6 ความรู้เกี่ยวกับภัยคุกคามประเภทต่าง ๆ เช่น ไวรัส , ช่องโหว่ของระบบ และการโจมตีทั่วไป

2.7 การป้องกันการโจมตีขั้นสูง

2.8 ความรู้เกี่ยวกับการเข้ารหัส

2.9 การบริหารจัดการความเสี่ยง

2.10 นโยบายการรักษาความปลอดภัย

## งานวิจัยที่เกี่ยวข้อง

ฐิตารีย์ จันทพันธ์ (2559) วิจัย เรื่อง “การศึกษาผลกระทบการรับรู้ความเสี่ยงในการใช้ระบุตำแหน่ง (Location - Based Services: LBS) บนสื่อสังคมออนไลน์ ต่อความเป็นส่วนตัวของผู้ใช้งานในกรุงเทพมหานคร” ผลการวิจัย พบว่า ปัจจัยการรับรู้ความเสี่ยงด้านความปลอดภัย และการรับรู้ความเสี่ยงด้านการไว้ใจ ในการใช้งานระบุตำแหน่ง (Location - Based Services: LBS) บนสื่อสังคมออนไลน์ ส่งผลกระทบต่อความเป็นส่วนตัวของผู้ใช้งานในเขตกรุงเทพมหานคร โดยที่ปัจจัยการรับรู้ด้านความเสี่ยงด้านความปลอดภัย ส่งผลกระทบต่อความเป็นส่วนตัวของผู้ใช้งานในเขตกรุงเทพมหานครมากที่สุด ไม่ส่งผลกระทบต่อความเป็นส่วนตัวของผู้ใช้งานในเขตกรุงเทพมหานคร

ปิยะภัสร์ โรจน์รัตนวาณิชย์ (2557) วิจัย เรื่อง “แนวทางการคุ้มครองข้อมูลใน Big Data : ความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูล” ผลการวิจัย พบว่า ยังไม่มีกฎหมายที่บัญญัติขึ้นเป็นการเฉพาะ เรื่องความเป็นส่วนตัว รวมถึงการรักษาความมั่นคงปลอดภัยของข้อมูลของผู้ใช้บริการต่างๆ แม้ว่าจะมีการนำกฎหมายที่มีผลบังคับใช้ในปัจจุบันไปใช้ในกรณีการละเมิดความเป็นส่วนตัวจากการใช้ Big Data ก็ตาม แต่ก็ยังไม่ได้บัญญัติไว้ครอบคลุมถึงการคุ้มครองความเป็นส่วนตัวและความปลอดภัยของข้อมูลในกรณี Big Data ดังนั้นผู้วิจัยจึงมีความเห็นว่า ควรเร่งให้มีการออกกฎหมายเพื่อคุ้มครองข้อมูลส่วนบุคคลที่มีอยู่ในความครอบครองของภาคเอกชนเป็นการทั่วไป และเพื่อเป็นการวางมาตรการในเชิงป้องกันการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคล และความปลอดภัยของข้อมูล และเพื่อระบุถึงสิทธิหน้าที่ของผู้ที่เกี่ยวข้องกับ Big Data ให้มีความชัดเจน แน่นอน ผู้เขียนเห็นว่าควรจะพยายามตีความกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลให้ ครอบคลุมมาถึงความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลกรณี Big Data ด้วยแล้วอาศัยอำนาจทางกฎหมายดังกล่าวออกกฎหมายลำดับรองเพื่อวางแนวทางในการคุ้มครองความเป็นส่วนตัวและความมั่นคงปลอดภัยของข้อมูลกรณี Big Data เป็นการเฉพาะ

อุบลวรรณ ภีระเป็ง (2558) วิจัยเรื่อง “การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ : ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ” ทั้งนี้งานวิจัยนี้มีจุดประสงค์เพื่อศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศว่าสามารถบังคับใช้กับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ ในฐานะเป็นวิธีการและปัจจัยในการสู้รบที่เกิดขึ้นใหม่ได้หรือไม่เพียงใด อนึ่ง กฎหมายมนุษยธรรมระหว่างประเทศเป็นกฎหมายระหว่างประเทศบังคับใช้เมื่อมีการสู้รบหรือสถานการณ์การขัดกันทางอาวุธเกิดขึ้นประกอบด้วยหลักเกณฑ์เกี่ยวกับปฏิบัติการทางทหาร รวมทั้งการให้ความคุ้มครองพลเรือน จากการศึกษาวิจัยพบว่าแม้ว่าการโจมตีทางไซเบอร์จะเป็นวิธีการและปัจจัยในการสู้รบใหม่ และไม่ปรากฏข้อบทที่เกี่ยวข้องกับการใช้เทคโนโลยีตามกฎหมายมนุษยธรรมระหว่างประเทศ แต่กฎหมายมนุษยธรรมระหว่างประเทศสามารถยืดหยุ่นครอบคลุมกับการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธอันเป็นการนำเอาเทคโนโลยีสารสนเทศและคอมพิวเตอร์หรือไซเบอร์มาใช้ในปฏิบัติการทางทหารและการสู้รบได้ อย่างไรก็ตาม ด้วยลักษณะ

ความเชื่อมต่อของเทคโนโลยีที่ใช้ในทางทหารและพลเรือน อีกทั้งการโจมตีทางไซเบอร์ยังเป็นการกระทำภายในห้วงไซเบอร์ที่ไม่มีลักษณะทางกายภาพก่อให้เกิดข้อท้าทายในบังคับใช้หลักการสำคัญตามกฎหมายมนุษยธรรมระหว่างประเทศ ไม่ว่าจะเป็นหลักการ แยกแยะเป้าหมาย หลักความ ได้สัดส่วนในการโจมตี หลักการใช้ความระมัดระวังในการโจมตีอย่างมีนัยสำคัญ จำเป็นจะต้องอาศัยความร่วมมือจากผู้ที่มีส่วนเกี่ยวข้องทั้งภาคประชาสังคม ภาครัฐ และความร่วมมือระหว่างประเทศในการพัฒนาแนวทางการรับมือการโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธที่จะนำไปสู่แนวทางปฏิบัติของรัฐที่ชัดเจนต่อไป เพื่อให้กฎหมายมนุษยธรรมระหว่างประเทศสามารถรองรับวิธีการและปัจจัยในการสู้รบใหม่ซึ่งมีความซับซ้อนของเทคโนโลยีสารสนเทศ และคอมพิวเตอร์ทวีขึ้นไปตามกาลเวลาได้อย่างมีประสิทธิภาพ ศิวลีย์ สิริโรจน์บริรักษ์ (2558) วิจัยเรื่อง “การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) ของกระทรวงกลาโหม” มีวัตถุประสงค์เพื่อศึกษานโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ศึกษามาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล และเพื่อเสนอแนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอรของกระทรวงกลาโหม ให้ได้มาตรฐานระดับสากล โดยการศึกษาครั้งนี้ใช้วิธีการสัมภาษณ์กลุ่มผู้ให้ข้อมูลสำคัญ (Key Informants) และการค้นคว้าข้อมูลจากเอกสารทางวิชาการต่าง ๆ ที่มีเนื้อหาเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม และมาตรฐานการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากลผลการศึกษา พบว่า

1. กรอบนโยบายยุทธศาสตร์ และการดำเนินงานดำเนินความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหม ได้แก่ พ.ร.บ.ว่าด้วยการจัดระเบียบราชการด้านเทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงกลาโหม พ.ศ.2551, นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกระทรวงกลาโหม พ.ศ.2554, ยุทธศาสตร์กระทรวงกลาโหมอิเล็กทรอนิกส์ (e-Defence), แผนแม่บท เทคโนโลยีสารสนเทศและการสื่อสารของกระทรวงกลาโหม ฉบับที่ 3 พ.ศ.2557 - 2561, การจัดตั้งศูนย์บัญชาการไซเบอร์ กระทรวงกลาโหม

2. มาตรฐานการดำเนินงานดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO 27001: 2005, มาตรฐาน FIPS PUB 200, มาตรฐาน NIST 800 - 14, มาตรฐาน COBIT, และมาตรฐาน IT BPM

3. แนวทางในการพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมให้ได้มาตรฐานในระดับสากล เชิงนโยบาย ได้แก่ ส่วนบังคับการ ต้องเปิดอัตรานายทหารสงครามข้อมูลข่าวสาร เพื่อดำเนินการตอบสนองต่อภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ (Cyber Threat) เป็นประเด็นปัญหาที่ทำให้ประเทศต่าง ๆ ทั่วโลก เกิดการตื่นตัวและตระหนักถึงปัญหา ดังจะเห็นได้จากปรากฏการณ์ที่ก่อให้เกิดความเปลี่ยนแปลงในโลกอาหรับ หรือที่รู้จักโดยทั่วไปว่าปรากฏการณ์ “Arab Spring” หรือ แม้แต่กลุ่มก่อการร้าย ISIS ซึ่งใช้เครือข่ายสังคมออนไลน์ เช่น Twitter, Facebook ฯลฯ เป็น เครื่องมือสำคัญในการปลุกระดมมวลชน เป็นต้น จากรายงานของ World Economic Forum แสดง ให้เห็นว่า ทั่วโลกกำลังวิตกกังวลกับภัยคุกคามความมั่นคงปลอดภัยไซเบอร์เป็นอย่างมาก โดยภัยคุกคามความมั่นคงปลอดภัยไซเบอร์ถูกจัดให้อยู่ในอันดับที่ 4 ใน 10 Trends ของโลก ประกอบกับ ผลการศึกษาของสถาบัน The Business Continuity Institute (BCI)

ซึ่งเป็นสถาบันอันดับหนึ่งของโลกด้านการบริหารความต่อเนื่องทางธุรกิจ ยังแสดงให้เห็นว่า Cyber Attack เป็นประเด็นอันดับต้น ๆ ที่องค์กร ให้ความสนใจมากที่สุด

วิภารัตน์ ปทักขินัง (2557) วิจัยเรื่อง “การพัฒนาระบบสารสนเทศสำหรับการประเมินระดับความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ ขององค์กร” พบว่า การวิจัยนี้มีวัตถุประสงค์เพื่อวิเคราะห์ความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์ การนำเสนอตัวแบบการประเมินความเสี่ยงและความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์และการพัฒนาระบบสารสนเทศสำหรับประเมินด้านความมั่นคงปลอดภัยไซเบอร์ ผู้วิจัยได้ใช้กรณีศึกษาของวิทยาลัยเทคโนโลยีสยาม และได้เก็บรวมรวบข้อมูลจากผู้ที่ทำหน้าที่เกี่ยวข้องกับไอซีทีเป็นกลุ่มตัวอย่าง ผลการวิจัยพบว่า องค์ประกอบความพร้อมด้านความมั่นคงปลอดภัยทางไซเบอร์จะประกอบไปด้วย 7 ด้าน ได้แก่

1. ด้านยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์
2. ด้านกฎระเบียบที่เกี่ยวข้อง
3. ด้านศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยทางไซเบอร์
4. ด้านการป้องกันอาญากรรมไซเบอร์
5. ด้านการพัฒนาด้านไซเบอร์
6. ด้านงบประมาณการวิจัย
7. ด้านความร่วมมือกับหน่วยงานอื่น ๆ

สำหรับตัวแบบการประเมิน ความเสี่ยงจะประกอบไปด้วย 4 ด้าน ได้แก่

1. กำหนดหัวข้อการบริหารจัดการความเสี่ยง
2. การวิเคราะห์ความเสี่ยง
3. การวางแผนการลดความเสี่ยง
4. การรายงานและการประเมินผล

สุธาเทพ รุณเรศ (2561) วิจัยเรื่อง “ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” การวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาปัจจัยทางด้านลักษณะทางประชากร ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ และความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต ผลการวิจัยพบว่า

1. ปัจจัยทางด้านลักษณทางประชากรด้านอายุ ระดับการศึกษา และรายได้ส่วนตัวต่อเดือน มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต แต่ปัจจัยทางด้านลักษณะทางประชากรด้านเพศไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต
2. ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต
3. ปัจจัยทางด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ต

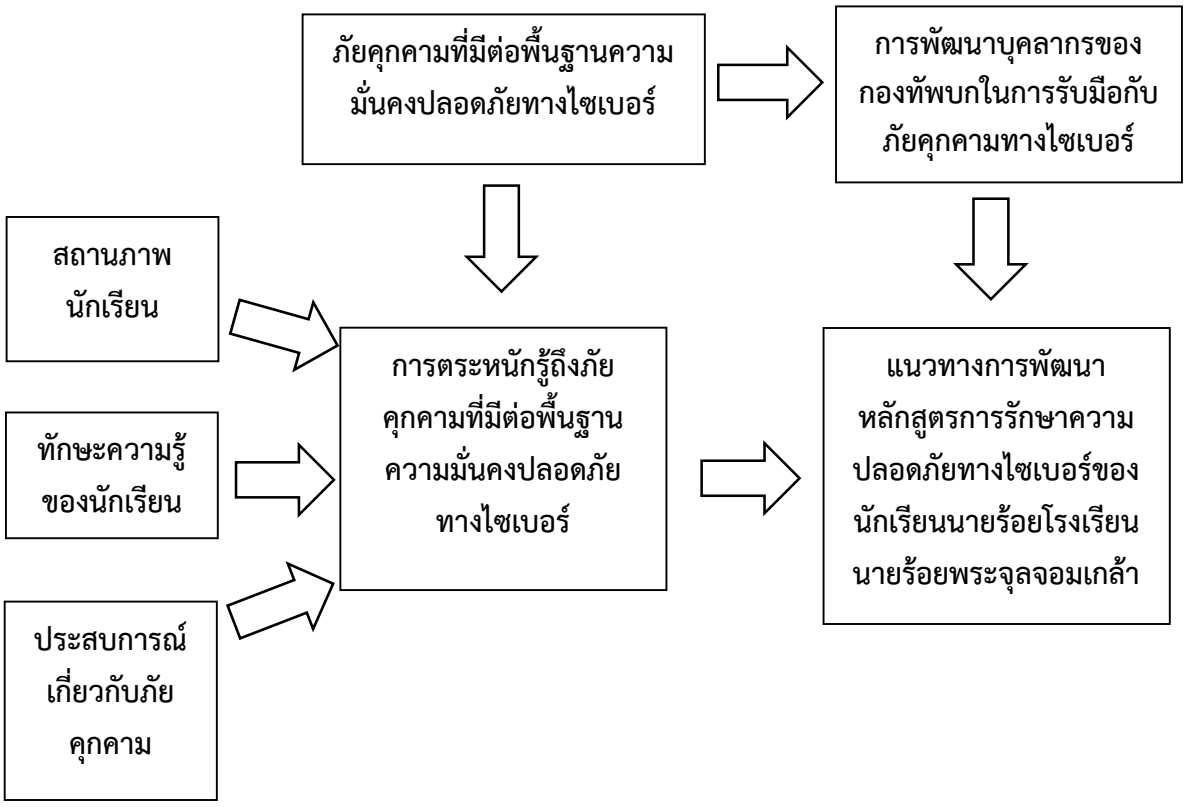
สุกัญญา ช้างแก้ว (2555) วิจัยเรื่อง “การเสริมสร้างความมั่นคงด้านเทคโนโลยีของกองทัพบก” การวิจัยนี้เป็นการนำเสนอแนวทางการเสริมสร้างความมั่นคงด้านเทคโนโลยีสารสนเทศกองทัพบก โดยมีวัตถุประสงค์การวิจัยเพื่อศึกษาภัยคุกคามด้านเทคโนโลยีสารสนเทศที่มีต่อกองทัพบก

จากผลการศึกษาพบว่า กองทัพบกยังขาดเครื่องมือ อุปกรณ์ในการรักษาความปลอดภัย ขาดหน่วยงานที่รับผิดชอบอย่างเป็นรูปธรรม ในด้านการใช้งานผู้ใช้มีการใช้งานผ่านเครือข่ายอินเทอร์เน็ตทำให้มีโอกาสเสี่ยงในการเกิดภัยคุกคามได้ง่าย และยังมีความรู้ความเข้าใจเกี่ยวกับภัยคุกคามค่อนข้างน้อย ผู้ดูแลระบบของหน่วยมีความชำนาญเกี่ยวกับการแก้ปัญหาภัยคุกคามค่อนข้างจำกัด การให้คำแนะนำช่วยเหลือยังไม่สามารถดำเนินการได้อย่างทั่วถึง เอกสารที่เกี่ยวข้องกับการรักษาความปลอดภัยมีไม่ครบทุกหน่วย ในภาพรวมกองทัพบกจึงมีความเสี่ยงต่อภัยคุกคามด้านไซเบอร์ค่อนข้างมาก แต่อย่างไรก็ตามผู้บังคับบัญชาหรือผู้บริหารหน่วยในทุกระดับ มีมุมมองที่ดีเกี่ยวกับการให้การสนับสนุนการดำเนินการเกี่ยวกับเทคโนโลยีสารสนเทศเป็นอย่างดี แต่มีข้อจำกัดในเรื่องของงบประมาณ

## กรอบแนวคิดของการวิจัย

ผู้วิจัยกำหนดกรอบแนวคิดในการศึกษาหัวข้อ “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” ดังนี้

แผนภาพที่ 2-1 กรอบแนวคิดการวิจัย




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

# บทที่ 3
# ระเบียบวิธีวิจัย

การศึกษาเรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” เป็นการศึกษาการวิจัยเชิงปริมาณ และเชิงคุณภาพ หรือแบบผสมผสาน (Mixed Method) โดยผู้วิจัยรวบรวมข้อมูลจากการทบทวนวรรณกรรม บทความวิชาการ หนังสือ เอกสารวิจัย และเอกสารอื่น ๆ ที่เกี่ยวข้อง รวมถึงสื่อออนไลน์ที่รวบรวมข้อมูลที่เชื่อถือได้ จากนั้นได้จัดทำแบบสอบถาม (Questionnaire) ในการเก็บรวบรวมข้อมูลความคิดเห็นของกลุ่มตัวอย่าง คือนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 จำนวน 300 นาย ให้กลุ่มตัวอย่างเป็นผู้ตอบแบบสอบถามด้วยตนเอง (Self Administered) เพื่อให้การดำเนินการวิจัยนำไปสู่วัตถุประสงค์ที่ตั้งไว้ โดยผู้วิจัยได้ดำเนินการศึกษาวิจัยตามขั้นตอน ดังนี้

1. การออกแบบการวิจัย
2. ประชากรและกลุ่มตัวอย่าง
3. เครื่องมือที่ใช้ในการวิจัย
4. การสร้างเครื่องมือวิจัย
5. ความเที่ยงตรงและความน่าเชื่อถือ
6. การเก็บรวบรวมข้อมูล
7. การวิเคราะห์ข้อมูล
8. สถิติที่ใช้ในการวิจัย

## การออกแบบการวิจัย

การดำเนินการวิจัยครั้งนี้ใช้วิธีวิทยาการวิจัยแบบผสม (Mixed Method) ประกอบด้วยการวิจัยเชิงปริมาณ (Quantitative Research) และการวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้การวิจัยเชิงปริมาณ เพื่อศึกษาปัจจัยความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 และใช้การวิจัยเชิงคุณภาพเพื่อศึกษาปัญหาและแนวทางในการพัฒนาการสร้างความตระหนักรู้ภัยคุกคามทางไซเบอร์ให้กับนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า โดยสรุปในการดำเนินการวิจัยดังนี้

### 1. การวิจัยเชิงปริมาณ

1.1 ศึกษารายละเอียดเกี่ยวกับ แนวคิด ทฤษฎี เนื้อหา จากเอกสารทางวิชาการ ตำรา วารสาร บทความทางวิชาการที่ เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

1.2 ดำเนินการสำรวจโดยใช้แบบสอบถาม คือ ลักษณะประชากร ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ และความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

**2. การวิจัยเชิงคุณภาพ**

2.1 ศึกษารายละเอียดเกี่ยวกับ แนวคิด ทฤษฎี เนื้อหา จากเอกสารทางวิชาการ ตำรา วารสาร บทความทางวิชาการที่เกี่ยวกับข้อแนวทางการทำวิจัยเชิงคุณภาพ

2.2 ดำเนินการสัมภาษณ์นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า โดยใช้แบบสัมภาษณ์แบบกึ่งโครงสร้าง (Semi-Structured Selection Interview) โดยทำการสัมภาษณ์พร้อมกับการทำวิจัยเชิงปริมาณ

## ประชากรและกลุ่มตัวอย่าง

**1. ประชากรที่นำมาศึกษาในงานครั้งนี้**

ประชากร คือ นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 ดังนี้

นักเรียนนายร้อยชั้นปีที่ 1 จำนวน 262 นาย
นักเรียนนายร้อยชั้นปีที่ 2 จำนวน 258 นาย
นักเรียนนายร้อยชั้นปีที่ 3 จำนวน 226 นาย
นักเรียนนายร้อยชั้นปีที่ 4 จำนวน 231 นาย
นักเรียนนายร้อยชั้นปีที่ 5 จำนวน 207 นาย

รวมนักเรียนนายร้อยพระจุลจอมเกล้า ที่ศึกษาในปี 2562 จำนวน 1,184 นาย

**2. การกำหนดขนาดกลุ่มตัวอย่าง**

ขนาดตัวอย่างในการวิจัยครั้งนี้ ได้คำนวณจากสูตรของ ทาโร ยามาเน (Taro Yamane, 1973)

จากสูตร $n = N/1+Ne^2$

เมื่อ n แทน ขนาดกลุ่มตัวอย่าง
N แทน ขนาดประชากร
e แทน ค่าคลาดเคลื่อนของการประมาณค่า กำหนดเป็น 0.05

การประเมินความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 มีประชากร จำนวน 1,184 นาย ผู้วิจัยกำหนดค่าคลาดเคลื่อนของการเลือกกลุ่มตัวอย่าง หรือค่าคลาดเคลื่อนของการประเมินค่าไว้ที่ร้อยละ 5 หรือ 0.05 ดังนั้นจะใช้กลุ่มตัวอย่างดังนี้

แทนค่าในสูตร $n = N/1+Ne^2$

จะได้ $n = 1184/1+(1184 * 0.05^2)$

$n = 298.9899$

จากการคำนวณจะได้ขนาดตัวอย่าง 298 นาย แต่ในการวิจัยครั้งนี้จะใช้ขนาดตัวอย่าง 300 นาย

**3. วิธีการสุ่มตัวอย่าง**

วิธีการสุ่มตัวอย่างได้ใช้การสุ่มตัวอย่างแบบไม่ใช่หลักความน่าจะเป็น (Non-Probability Sampling) ด้วยวิธีการสุ่มตัวอย่างแบบบังเอิญ (Accidental Sampling) และวิธีการสุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling)

1. การสุ่มตัวอย่างโดยไม่ใช้ความน่าจะเป็น (Non-probability sampling) เป็นการเลือกตัวอย่างโดยไม่คำนึงว่าตัวอย่างแต่ละหน่วยมีโอกาสถูกเลือกมากน้อยเพียงไร

2. การเลือกกลุ่มตัวอย่างแบบบังเอิญ (Accidental sampling) เป็นการเลือกกลุ่มตัวอย่างเพื่อให้ได้จำนวนตามต้องการโดยไม่มีหลักเกณฑ์ กลุ่มตัวอย่างจะเป็นใครก็ได้ที่สามารถให้ข้อมูล

3. วิธีการสุ่มตัวอย่างแบบสโนว์บอล (Snowball Sampling) เป็นการบอกต่อของผู้ตอบแบบสอบถามจนกว่าจะได้จำนวนที่ต้องการ

## เครื่องมือที่ใช้ในการวิจัย

การดำเนินการวิจัยครั้งนี้ใช้วิธีวิทยาการวิจัยแบบผสม (Mixed Method) ซึ่งใช้แบบสอบถามเป็นเครื่องมือในการวิจัยเชิงปริมาณ (Quantitative Research) และใช้แบบสัมภาษณ์เป็นเครื่องมือในการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีรายละเอียดของเครื่องมือทั้ง 2 ประเภทดังนี้

1. การวิจัยเชิงปริมาณใช้แบบสอบถามเพื่อศึกษาปัจจัยของความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” ใช้แบบสอบถาม (Questionnaire) ในการเก็บรวบรวมข้อมูล ข้อคิดเห็นของกลุ่มตัวอย่าง สอบถามกลุ่มตัวอย่างแบบคำถามลักษณะปลายปิด (Close end questionnaire) กลุ่มตัวอย่างเป็นผู้ตอบแบบสอบถามด้วยตนเอง (Self-Administered) ประกอบไปด้วยข้อคำถาม จำนวน 3 ตอน ดังนี้

ตอนที่ 1 ลักษณะประชากร ประกอบด้วยคำถาม 2 ข้อ ได้แก่

1. สถานภาพของนักศึกษา : ชั้นปีการศึกษาของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า คือ

1.1 ชั้นปีที่ 1
1.2 ชั้นปีที่ 2
1.3 ชั้นปีที่ 3
1.4 ชั้นปีที่ 4
1.5 ชั้นปีที่ 5

2. ทักษะความรู้ของนักศึกษา : หลักสูตรโรงเรียนนายร้อยพระจุลจอมเกล้า พ.ศ.2562 แบ่งออกเป็น 8 กลุ่ม คือ

2.1 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล
2.2 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร
2.3 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ

2.4 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา

2.5 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมแผนที่

2.6 หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์

2.7 หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี

2.8 หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา

ตอนที่ 2 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน 10 ข้อ ได้แก่

1.นักเรียนเคยได้รับผลกระทบจากไวรัสที่ทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย

2.นักเรียนเคยถูกก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ

3. นักเรียนติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวเข้ามา

4. นักเรียนถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของนักเรียนได้โดยไม่รู้ตัว

5. นักเรียนถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์

6. นักเรียนโดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน

7. นักเรียนไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นจะได้รับข้อความ “เรียกค่าไถ่”

8. นักเรียนถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ

9. นักเรียนเคยได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง

10. นักเรียนเคยได้รับโฆษณาที่ไม่พึงประสงค์จะได้รับ

เกณฑ์การให้คะแนนคือ

มีประสบการณ์ = 1

ไม่มีประสบการณ์ = 0

หลังจากนั้นจะรวมคะแนนทั้ง 10 ข้อ เป็นคะแนนรวมประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อนำไปวิเคราะห์ต่อไป

อย่างไรก็ตามได้นำคะแนนรวมนั้นมาแบ่งระดับประสบการณ์ เกี่ยวกับภัยคุกคามทางไซเบอร์ เป็น 3 ระดับดังนี้

0-3 คะแนน หมายถึง มีประสบการณ์น้อย

4-6 คะแนน หมายถึง มีประสบการณ์ปานกลาง

7-10 คะแนน หมายถึง มีประสบการณ์มาก

ตอนที่ 3 ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ แบ่งเป็น 3ด้าน คือ ความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการจารกรรมข้อมูล, ความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้าย และความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม โดยแต่ละด้านประกอบด้วยคำถาม 10 ข้อ รวมเป็น 30 ข้อ โดยแบบสอบถามมีลักษณะเป็นมาตราส่วนประเมินค่า (Rating Scale) ตามแบบ Likert วัดค่าเป็น 5 ระดับ คือ ไม่เคย, น้อย,

ปานกลาง, มาก, มากที่สุด โดยการตอบคำถาม ขอให้นักเรียนตอบตามที่ตนเองปฏิบัติจริงไม่จำเป็นต้องตามทฤษฎี หรือข้อกำหนดด้านการรักษาความปลอดภัย

1. ความตระหนักรู้ภัยคุกคามจากการจารกรรมข้อมูล

1.1 นักเรียนตั้งรหัสผ่านมากกว่า 8 ตัวอักษรขึ้นไปหรือไม่ และนักเรียนตั้งรหัสผ่านที่ประกอบด้วย ตัวอักษรตัวเล็ก (Lowercase Letter) ตัวใหญ่ (Uppercase Letter) ตัวเลข (Number) และอักษรพิเศษ (Special Letter ตัวอย่างเช่น @,$,&,฿ เป็นต้น) หรือไม่

1.2 นักเรียนจดรหัสผ่านไว้ในที่ ๆ นักเรียนสามารถเรียกดูได้หรือไม่ เช่น ในกระดาษ หรือในโทรศัพท์มือถือ

1.3 นักเรียนใช้รหัสผ่านเดียวกันในทุกโปรแกรมหรือไม่

1.4 นักเรียนเปลี่ยนรหัสผ่านบ่อยหรือไม่

1.5 นักเรียนโพสต์ข้อมูลส่วนตัว เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ วันเดือนปีเกิด บนสื่อสังคมออนไลน์หรือไม่

1.6 นักเรียนใช้ wifi สาธารณะในการเปิดดูข้อมูลส่วนตัว หรือข้อมูลที่มีความสำคัญเช่น ข้อมูลทางการเงินหรือไม่

1.7 นักเรียนออกจากระบบ (Log out) ทุกครั้งที่ใช้งานโปรแกรมหรือไม่

1.8 เมื่อเข้าเว็บไซต์ นักเรียนเลือก “Keep me logged in” หรือ “Remember me” หรือไม่

1.9 การทำธุรกรรมทางการเงินบนอินเทอร์เน็ต นักเรียนได้ตรวจสอบ URL ของเว็บไซต์ ว่าเริ่มด้วย https:// หรือไม่

1.10 หากธนาคารที่นักเรียนใช้บริการอยู่เป็นประจำ ได้ส่งจดหมายอิเล็กทรอนิกส์ (E-mail) มายังนักเรียน เพื่อแจ้งการปรับปรุงระบบรักษาความปลอดภัยระหว่างนักเรียนและธนาคารให้ดียิ่งขึ้นโดยให้นักเรียนเข้าระบบ (Login) ด้วยการกรอกข้อมูลผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อดำเนินการกรอกข้อมูลในการปรับปรุงระบบ นักเรียนจะดำเนินการหรือไม่

เกณฑ์การให้คะแนน

ข้อ 1.1, 1.4, 1.7, 1.9

| | |
|---|---|
| ไม่ | = 1 |
| น้อย | = 2 |
| ปานกลาง | = 3 |
| มาก | = 4 |
| มากที่สุด | = 5 |

ข้อ 1.2, 1.3, 1.5, 1.8, 1.10

| | |
|---|---|
| ไม่ | = 5 |
| น้อย | = 4 |
| ปานกลาง | = 3 |
| มาก | = 2 |
| มากที่สุด | = 1 |

หลังจากนั้นจะเฉลี่ยคะแนนทั้ง 10 ข้อ เป็นคะแนนเฉลี่ยความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการจารกรรมข้อมูล เป็น 5 ระดับดังนี้

คะแนนเฉลี่ย 1.00 – 1.49 หมายถึง ตระหนักน้อยที่สุด
คะแนนเฉลี่ย 1.50 – 2.49 หมายถึง ตระหนักน้อย
คะแนนเฉลี่ย 2.50 – 3.49 หมายถึง ตระหนักปานกลาง
คะแนนเฉลี่ย 3.50 – 4.49 หมายถึง ตระหนักมาก
คะแนนเฉลี่ย 4.50 – 5.00 หมายถึง ตระหนักมากที่สุด

2. ความตระหนักรู้ภัยคุกคามไซเบอร์จากโปรแกรมประสงค์ร้าย

นักเรียนจะดาวน์โหลดโปรแกรมฟรีบนอินเทอร์เน็ตมาติดตั้งบนเครื่องคอมพิวเตอร์

2.1 นักเรียนติดตั้งโปรแกรมป้องกันไวรัสที่ระบบคอมพิวเตอร์หรือไม่

2.2 นักเรียนอัพเดตโปรแกรม, แอพพลิเคชันอย่างสม่ำเสมอหรือไม่

2.3 ก่อนใช้งานอุปกรณ์สำรองข้อมูล นักเรียนทำการสแกนไวรัสทุกครั้งหรือไม่

2.4 หากนักเรียนบังเอิญพบอุปกรณ์อิเล็กทรอนิกส์ เช่น ทรัมป์ไดรฟ์ หรือ External Hard Disk ซึ่งไม่ทราบว่าเป็นของผู้ใด นักเรียนจะนำอุปกรณ์เหล่านี้ไปเปิดดูบนเครื่องคอมพิวเตอร์หรือไม่

2.5 นักเรียนเปิดไฟล์แนบ (Attachment) ในจดหมายอิเล็กทรอนิกส์ (email) จากผู้ที่ไม่รู้จัก หรือไม่ทราบแหล่งที่มาหรือไม่

2.6 นักเรียนคลิกไปยังลิงค์ (Link) ของผู้ไม่รู้จักหรือไม่รู้จักแหล่งที่มาหรือไม่

2.7 นักเรียนสังเกตการทำงานของเครื่องคอมพิวเตอร์เสมอ เช่น การทำงานที่ช้าลง การรับ-ส่งข้อมูลที่ช้าลง และตรวจสอบว่ามีความผิดปกติหรือไม่

2.8 นักเรียนมีการสำรองข้อมูลสำคัญให้พอเพียงพร้อมใช้งานอยู่เสมอหรือไม่

2.9 นักเรียนกดดูโฆษณา เมื่อขึ้นมาบนจอคอมพิวเตอร์ (Pop-up Ads) หรือไม่

เกณฑ์การให้คะแนน

ข้อ 2.2 , 2.3 , 2.4 , 2.8

ไม่ = 1
น้อย = 2
ปานกลาง = 3
มาก = 4
มากที่สุด = 5

ข้อ 2.1 , 2.5 , 2.6 , 2.7 , 2.10

ไม่ = 5
น้อย = 4
ปานกลาง = 3
มาก = 2
มากที่สุด = 1

หลังจากนั้นจะเฉลี่ยคะแนนทั้ง 10 ข้อ เป็นคะแนนเฉลี่ยความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้ายเป็น 5 ระดับดังนี้

คะแนนเฉลี่ย 1.00 – 1.49 หมายถึง ตระหนักน้อยที่สุด
คะแนนเฉลี่ย 1.50 – 2.49 หมายถึง ตระหนักน้อย
คะแนนเฉลี่ย 2.50 – 3.49 หมายถึง ตระหนักปานกลาง
คะแนนเฉลี่ย 3.50 – 4.49 หมายถึง ตระหนักมาก
คะแนนเฉลี่ย 4.50 – 5.00 หมายถึง ตระหนักมากที่สุด

3. ความตระหนักรู้ภัยคุกคามทางไซเบอร์ จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม

3.1 เมื่อได้รับจดหมายลูกโซ่ หรือข้อมูลข่าวสาร นักเรียนส่งต่อหรือทำการแชร์ข้อมูลโดยไม่มีการตรวจสอบความถูกต้องหรือไม่

3.2 หากนักเรียนเชื่อหรือปฏิบัติตามข้อมูลบนสื่อออนไลน์ นักเรียนได้ทำการหาข้อมูลวิเคราะห์ และสรุปผลหาความถูกต้องก่อนที่จะเชื่อหรือปฏิบัติตามหรือไม่

3.3 นักเรียนนำภาพหรือข้อมูลของผู้อื่นที่ได้จากการคัดลอก (Copy) หรือ ดาวน์โหลด (Download) โดยไม่ได้รับอนุญาตมาโพสต์โดยไม่ได้ให้เครดิตเจ้าของภาพหรือไม่

3.4 นักเรียนเคยกล่าวถึงผู้อื่นให้ได้รับความอับอายเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์หรือไม่

3.5 นักเรียนเคยใช้ข้อความที่หยาบคายด่าว่าผู้อื่นผ่านทางไซเบอร์หรือไม่

3.6 นักเรียนเคยล้อเลียนรูปร่างหน้าตาของผู้อื่นผ่านทางไซเบอร์หรือไม่

3.7 นักเรียนเคยเผยแพร่ข่าวลือในทางลบของผู้อื่นผ่านทางไซเบอร์หรือไม่

3.8 นักเรียนเคยนำข้อมูลส่วนบุคคลของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์หรือไม่

3.9 นักเรียนเคยลบรายชื่อบุคคลที่ไม่ชอบออกจากลุ่มสนทนาทางไซเบอร์หรือไม่

3.10 นักเรียนเคยกดดันให้บุคคลที่ไม่ชอบให้ออกจากกลุ่มสนทนาทางไซเบอร์หรือไม่

เกณฑ์การให้คะแนน

ข้อ 3.2

| | |
|---|---|
| ไม่ | = 1 |
| น้อย | = 2 |
| ปานกลาง | = 3 |
| มาก | = 4 |
| มากที่สุด | = 5 |

ข้อ อื่น ๆ

| | |
|---|---|
| ไม่ | = 5 |
| น้อย | = 4 |
| ปานกลาง | = 3 |
| มาก | = 2 |
| มากที่สุด | = 1 |

หลังจากนั้นจะเฉลี่ยคะแนนทั้ง 10 ข้อ เป็นคะแนนเฉลี่ยความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสมเป็น 5 ระดับดังนี้

| | | | |
|---|---|---|---|
| คะแนนเฉลี่ย | 1.00 – 1.49 | หมายถึง | ตระหนักน้อยที่สุด |
| คะแนนเฉลี่ย | 1.50 – 2.49 | หมายถึง | ตระหนักน้อย |
| คะแนนเฉลี่ย | 2.50 – 3.49 | หมายถึง | ตระหนักปานกลาง |
| คะแนนเฉลี่ย | 3.50 – 4.49 | หมายถึง | ตระหนักมาก |
| คะแนนเฉลี่ย | 4.50 – 5.00 | หมายถึง | ตระหนักมากที่สุด |

## ความเที่ยงตรงและความน่าเชื่อถือ

แบบสอบถามที่ผู้วิจัยสร้างขึ้นจะนำมาทดสอบความเที่ยงตรง (Validity) และความน่าเชื่อถือ (Reliability) โดยผู้วิจัยได้นำร่างแบบสอบถามที่สร้างขึ้นให้อาจารย์ที่ปรึกษา และผู้เชี่ยวชาญการรักษาความปลอดภัยทางไซเบอร์ตรวจสอบความเที่ยงตรง และความน่าเชื่อถือเชิงเนื้อหา และนำข้อคิดเห็นของอาจารย์ที่ปรึกษาและผู้เชี่ยวชาญมาปรับแก้ก่อนนำไปทดสอบความน่าเชื่อถือและเก็บข้อมูลจริงต่อไป

## การเก็บรวบรวมข้อมูล

งานศึกษาเรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” ได้ศึกษาขั้นตอนในการเก็บรวบรวมข้อมูลดังต่อไปนี้

1. ข้อมูลปฐมภูมิ (Primary Data) คือ ข้อมูลที่ได้จากแบบสอบถามออนไลน์ (Online Questionnaire) ถึงปัจจัย 4 ด้าน ได้แก่ ด้านลักษณะทางประชากร ด้านประสบการณ์ เกี่ยวกับภัยคุกคามทางไซเบอร์ ด้านความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ และด้านความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ โดยเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่างของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

2. ข้อมูลทุติยภูมิ (Secondary Data) คือข้อมูลที่ได้จากแหล่งที่รวบรวมข้อมูลไว้แล้ว หรือหน่วยงานที่มีการบันทึกทำการรวบรวมสถิติต่าง ๆ หรือเรียบเรียงไว้เรียบร้อยแล้ว สามารถนำข้อมูลเหล่านั้นมาใช้อ้างอิงได้ ผู้วิจัยได้ทำการเก็บรวบรวมจากการทบทวนวรรณกรรม แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง รวมทั้งการสืบค้นทางอินเทอร์เน็ตจากเว็บไซต์ที่เกี่ยวข้องกับความตระหนักถึงภัยคุกคามทางไซเบอร์ เพื่อเป็นข้อมูลประกอบการวิเคราะห์งานวิจัย

## การวิเคราะห์ข้อมูล

การดำเนินการวิจัยครั้งนี้ใช้แบบสอบถามเป็นเครื่องมือในการวิจัยเชิงปริมาณ (Quantitative Research) และใช้แบบสัมภาษณ์เป็นเครื่องมือในการวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีวิธีการวิเคราะห์ข้อมูลในการวิจัยดังนี้

1. การวิเคราะห์ข้อมูลในการวิจัยเชิงปริมาณ ผู้วิจัยได้ดำเนินการวิเคราะห์ข้อมูลด้วยคอมพิวเตอร์ โดยใช้โปรแกรม (Statistical Package for Social Science - SPSS) ซึ่งดำเนินการตามขั้นตอนดังนี้

1.1 แบบสอบถามตอนที่ 1 เกี่ยวกับข้อมูลทั่วไปของผู้ตอบแบบสอบถาม โดยทำการวิเคราะห์แยกตามชั้นปีการศึกษาของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า และหลักสูตรที่เรียนที่เปิดสอนของโรงเรียนนายร้อยพระจุลจอมเกล้า จำนวน 8 หลักสูตร

1.2 แบบสอบถามตอนที่ 2 วิเคราะห์เกี่ยวกับประสบการณ์ด้านภัยคุกคามของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า โดยหาค่าเฉลี่ยเลขคณิต (Arithmetic Mean) และค่าส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) เพื่อแบ่งคะแนนเป็นช่วง ๆ แต่ละช่วงมีความหมายดังนี้

0-3 คะแนน หมายถึง มีประสบการณ์น้อย

4-6 คะแนน หมายถึง มีประสบการณ์ปานกลาง

7-10 คะแนน หมายถึง มีประสบการณ์มาก

1.3 แบบสอบถามตอนที่ 3 วิเคราะห์เกี่ยวกับความตระหนักรู้ภัยคุกคามด้านไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปีการศึกษา 2562

| | | | |
|---|---|---|---|
| คะแนนเฉลี่ย | 1.00 – 1.49 | หมายถึง | ตระหนักน้อยที่สุด |
| คะแนนเฉลี่ย | 1.50 – 2.49 | หมายถึง | ตระหนักน้อย |
| คะแนนเฉลี่ย | 2.50 – 3.49 | หมายถึง | ตระหนักปานกลาง |
| คะแนนเฉลี่ย | 3.50 – 4.49 | หมายถึง | ตระหนักมาก |
| คะแนนเฉลี่ย | 4.50 – 5.00 | หมายถึง | ตระหนักมากที่สุด |

จากนั้นหาค่าทดสอบเอฟ (F-test) เพื่อเปรียบเทียบความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ ตามปัจจัยด้านชั้นปีการศึกษาหลักสูตรการศึกษา และประสบการณ์ด้านภัยคุกคาม ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปีการศึกษา 2562 โดยทำการวิเคราะห์ความแปรปรวนทางเดียว (One-way ANOVA) ว่ามีความแตกต่างอย่างมีนัยสำคัญทางสถิติ (0.05) หรือไม่

2. การวิเคราะห์ข้อมูลในการวิจัยเชิงคุณภาพ ผู้วิจัยดำเนินการวิเคราะห์ข้อมูลซึ่งดำเนินตามขั้นตอนดังนี้

2.1 ตรวจความถูกต้องของข้อมูล

2.2 จำแนกและจัดระบบข้อมูล เป็นการนำข้อมูลที่ได้มาจำแนกและจัดหมวดหมู่ออกให้เป็นระบบ

2.3 วิเคราะห์ข้อมูลโดยการตีความสร้างข้อสรุปแบบอุปนัย (Analytic Induction) เป็นการนำข้อมูลที่ได้จากเหตุการณ์ต่าง ๆ ที่เกิดขึ้นมาวิเคราะห์เพื่อหาบทสรุปร่วมกันของเรื่องนั้น

2.4 นำเสนอข้อมูลเป็นข้อความแบบบรรยาย

## สถิติที่ใช้ในการวิจัย

สถิติที่ใช้ในการวิจัยจะใช้สถิติการวิเคราะห์ข้อมูลที่ได้รับจากการเก็บรวบรวมข้อมูลที่ผู้วิจัยได้จากกลุ่มตัวอย่างของงานวิจัย “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” โดยจะนำข้อมูลที่ได้มาวิเคราะห์ประมวลผลทางสถิติ และแบ่งการวิเคราะห์ข้อมูลได้ 2 ประเภท ดังต่อไปนี้

**1. สถิติเชิงพรรนา (Descriptive Statistics)** คือการนำข้อมูลที่เก็บได้มาจากกลุ่มตัวอย่างมาแสดงรายละเอียดของข้อมูลเพื่อที่จะอธิบายค่าของข้อมูล โดยแจกแจงความถี่ (Frequency) แบบค่าร้อยละ (Percentage) แบบคำนวนค่าเฉลี่ย (Mean) และแบบค่าเบี่ยงเบนมาตรฐาน (Standard Deviation) ในการพรรนาข้อมูลของกลุ่มตัวอย่างเกี่ยวกับลักษณะทางประชากร ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ และความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์

1.1 หาค่าเฉลี่ยเลขคณิต (Arithmetic Mean) โดยใช้

$\bar{x}. = \sum x / n$

เมื่อ $\bar{x}.$ แทน ค่าเฉลี่ยเลขคณิต

$\sum x$ แทน ผลรวมของคะแนนทั้งหมด

n แทน จำนวนกลุ่มตัวอย่างที่ตอบแบบสอบถาม

1.2 หาค่าความเบี่ยงเบนมาตรฐาน (Standard Deviation) ใช้สูตร

$$SD = \sqrt{\frac{\sum_{i-1}^{n}(x_i - \bar{x})^2}{n-1}}$$

เมื่อ SD แทน ค่าเบี่ยงเบนมาตรฐาน

$\bar{x}.$ แทน ผลรวมของคะแนนแต่ละตัวยกกำลังสอง

$X_i$ แทน ผลรวมของคะแนนทั้งหมดยกกำลังสอง

n แทน จำนวนกลุ่มตัวอย่างที่ตอบแบบสอบถาม

**2. สถิติเชิงอนุมาน (Inferential Statistics)** คือการนำข้อมูลที่ได้จากกลุ่มตัวอย่างมาทดสอบหาความสัมพันธ์ระหว่างตัวแปรอิสระ (Independent Variables) กับตัวแปรตาม (Dependent Variables) โดยการเปรียบเทียบแบบพหุคูณ เมื่อพบว่าค่าเฉลี่ยมีความแตกต่างกันอย่างมีนัยสำคัญทางสถิติโดยใช้ Independent Samples Oneway ANOVA และ Pearson Correlation ในการทดสอบสมมติฐาน

$$F = \frac{\bar{x}_1 - \bar{x}_2}{ms_w\left[\frac{1}{n_i}+\frac{1}{n_j}\right](k-1)}$$

เมื่อ F แทนค่าสถิติในการแจกแจงแบบเอฟ

$\bar{x}_1 - \bar{x}_2$ แทนค่าเฉลี่ยของข้อมูลกลุ่มตัวอย่างที่นำมาเปรียบเทียบ

$MS_w$ แทนค่าความแปรปรวนในกลุ่ม

$n_i$ $n_j$ แทนขนาดของข้อมูลกลุ่มตัวอย่างที่นำมาเปรียบเทียบ

k แทนจำนวนกลุ่มที่ศึกษา

# บทที่ 4
# ผลการวิจัย

การวิจัยเรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” เป็นการวิจัยเชิงปริมาณ (Quantities Research) โดยใช้แบบสอบถาม (Questionnaires) เป็นเครื่องมือในการเก็บรวบรวมข้อมูล ทำการแจกแบบสอบถามให้กับนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 จำนวน 5 ชั้นปี ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลและได้เสนอการวิเคราะห์ ข้อมูลผลการวิจัย แบ่งเป็น 3 ตอน ดังนี้

1. ข้อมูลลักษณะของประชากร
2. ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์
3. ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

สัญลักษณ์ที่ใช้ในการวิเคราะห์ข้อมูล

| | | |
|---|---|---|
| $\bar{x}$. | หมายถึง | ค่าเฉลี่ยเลขคณิต (Mean) |
| S.D. | หมายถึง | ค่าเฉลี่ยส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) |
| S.S | หมายถึง | ผลบวกกำลังสอง (Sum of Squares) |
| Df | หมายถึง | องศาอิสระ (Degree of Freedom) |
| MS | หมายถึง | ผลบวกกำลังสองเฉลี่ย (Sum of Squares) |
| F | หมายถึง | ค่าสถิติทดลอง F (F-value) |
| p | หมายถึง | ค่าความน่าจะเป็นทางสถิติ (p-value) |
| Sig | หมายถึง | ระดับนัยสำคัญ (Level of significance) |

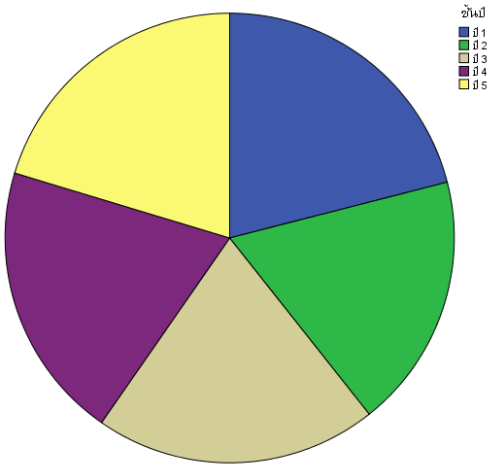
## ข้อมูลลักษณะของประชากร

ตารางที่ 4-1 จำนวนและค่าร้อยละของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าแยกตามชั้นปี

| ชั้นปี | จำนวน (คน) | ร้อยละ |
|---|---|---|
| 1 | 63 | 21 |
| 2 | 55 | 18.3 |
| 3 | 61 | 2.03 |
| 4 | 60 | 20.0 |
| 5 | 61 | 20.3 |
| รวม | 300 | 100 |

ที่มา : www.crma.ac.th/edu/EDU.pdf

แผนภาพที่ 4-1 แสดงจำนวน ร้อยละของลักษณะประชากรของผู้ตอบแบบสอบถามในแต่ละชั้นปี




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

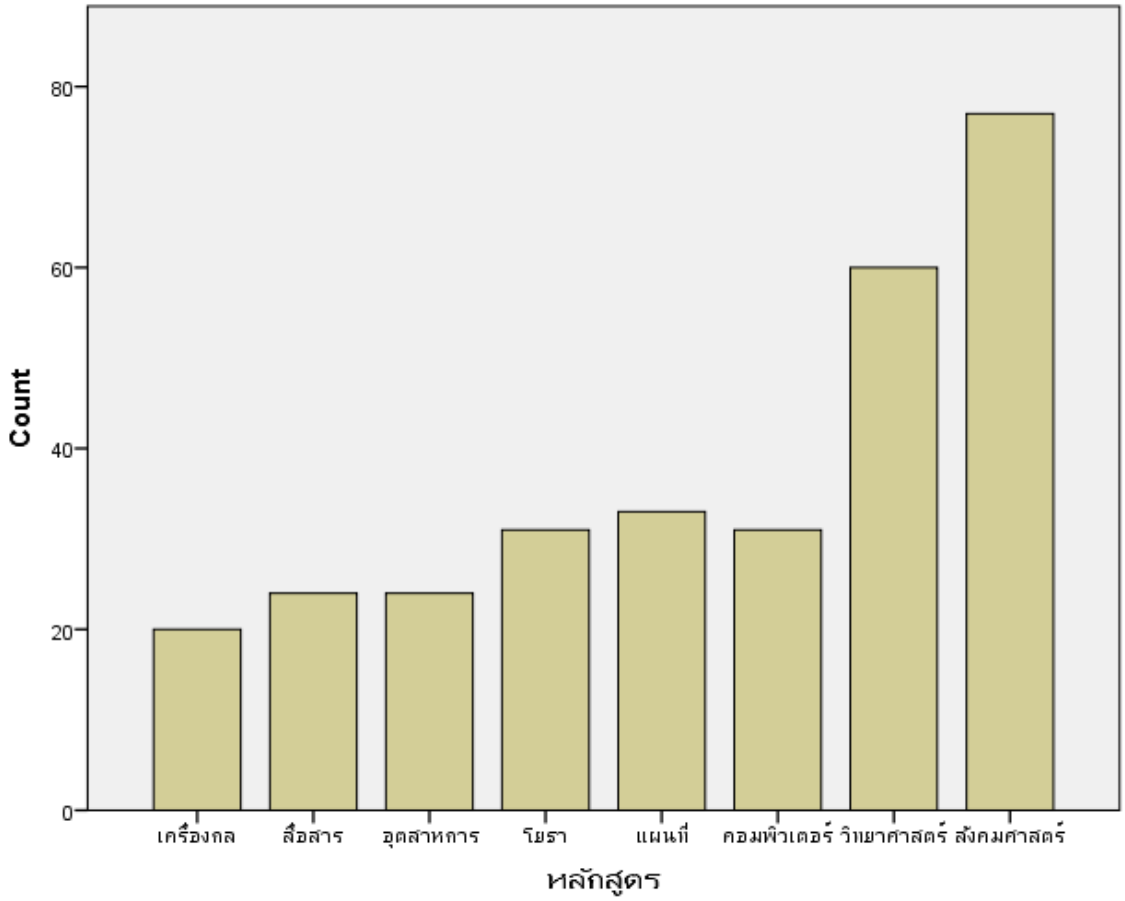
จากตารางที่ 4-1 และ แผนภาพที่ 4-1 พบว่าผู้ตอบแบบสอบถามจำนวน แต่ละชั้นปีมีจำนวนใกล้เคียงกัน โดยชั้นปีที่ 1 จำนวน 63 นาย คิดเป็นร้อยละ 21 ชั้นปีที่ 2 จำนวน 55 นาย คิดเป็นร้อยละ 18.3 ชั้นปีที่ 3 จำนวน 61 นาย คิดเป็นร้อยละ 20.3 ชั้นปีที่ 4 จำนวน 60 นาย คิดเป็นร้อยละ 20 และชั้นปีที่ 5 จำนวน 61 นาย คิดเป็นร้อยละ 20.3 ตามลำดับ

ตารางที่ 4-2 จำนวนและค่าร้อยละของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าที่ศึกษาอยู่ในหลักสูตร

| หลักสูตร | จำนวน (นาย) | ร้อยละ |
|---|---|---|
| วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล | 20 | 6.7 |
| วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร | 24 | 8.0 |
| วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมอุตสาหการ | 24 | 8.0 |
| วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมโยธา | 31 | 10.3 |
| วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมแผนที่ | 33 | 11 |
| วิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ | 31 | 10.3 |
| วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี | 60 | 20 |
| ศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา | 77 | 25.7 |
| รวม | 300 | |

ที่มา : www.crma.ac.th/edu/EDU.pdf

แผนภาพที่ 4-2 แสดงจำนวน ร้อยละของลักษณะประชากรของผู้ตอบแบบสอบถามในแต่ละหลักสูตร




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-2 และแผนภาพที่ 4-2 พบว่าผู้ตอบแบบสอบถามส่วนมากศึกษาหลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา มีจำนวน 77 นาย คิดเป็นร้อยละ 25.7 รองลงมาคือหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี จำนวน 60 นาย คิดเป็นร้อยละ 20 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมแผนที่ จำนวน 33 นาย คิดเป็นร้อยละ 11 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมโยธา และหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ มีผู้ตอบแบบสอบถามจำนวนเท่ากันคือ 31 นาย คิดเป็นร้อยละ 10.3 วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร และวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมอุตสาหการ มีผู้ตอบแบบสอบถามเท่ากันคือ 24 นาย คิดเป็นร้อยละ 8 และวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล มีผู้ตอบแบบสอบถามน้อยที่สุดคือ 20 นาย คิดเป็นร้อยละ 6.7 ตามลำดับ

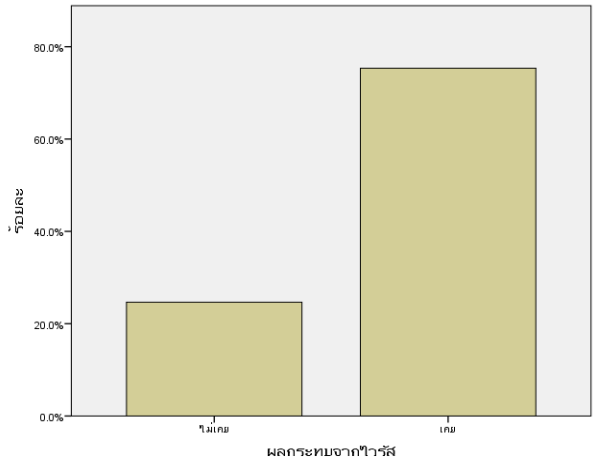
## ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

ตารางที่ 4-3 จำนวนร้อยละของผู้ตอบแบบสอบถามที่มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

| ลำดับ | เหตุการณ์ | ประสบการณ์ | | | | รวม |
|---|---|---|---|---|---|---|
| | | เคย | ร้อยละ | ไม่เคย | ร้อยละ | |
| 1. | นักเรียนเคยได้รับผลกระทบจากไวรัสที่ทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย | 226 | 75.3 | 74 | 24.7 | 300 |
| 2. | นักเรียนเคยถูกการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ | 191 | 63.7 | 109 | 36.3 | 300 |
| 3. | นักเรียนเคยติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวเข้ามา | 198 | 66 | 102 | 34 | 300 |
| 4. | นักเรียนเคยถูกผู้อื่นเข้ามาใช้งานคอมพิวเตอร์ของนักเรียนได้โดยไม่รู้ตัว | 117 | 39 | 183 | 61 | 300 |
| 5. | นักเรียนถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์ | 121 | 40.3 | 179 | 59.7 | 300 |
| 6. | นักเรียนเคยถูกขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน | 78 | 26 | 222 | 74.0 | 300 |
| 7. | นักเรียนไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นจะได้รับข้อความ “เรียกค่าไถ่” | 65 | 21.7 | 235 | 78.3 | 300 |
| 8. | นักเรียนเคยถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ | 150 | 50 | 150 | 50 | 300 |
| 9. | นักเรียนเคยได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง | 185 | 61.7 | 115 | 38.3 | 300 |
| 10. | นักเรียนเคยได้รับโฆษณาที่ไม่พึงประสงค์จะได้รับ | 237 | 79 | 63 | 21 | 300 |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

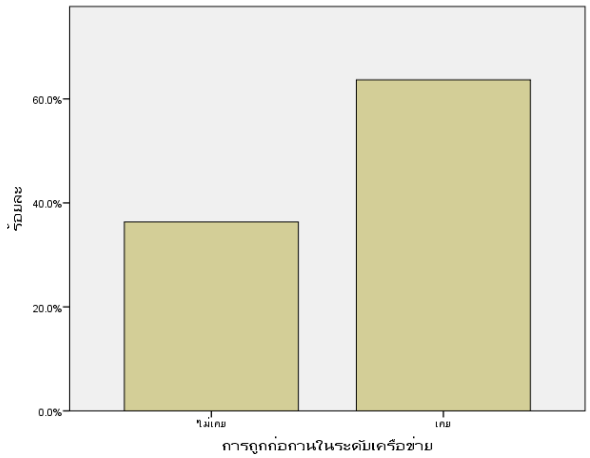
แผนภาพที่ 4-3 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่เคยได้รับผลกระทบจากไวรัสที่ทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากแผนภาพที่ 4-3 แสดงผู้มีประสบการณ์ภัยคุกคามทางไซเบอร์จากไวรัสคอมพิวเตอร์ที่ทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหายมีจำนวน 226 นาย คิดเป็นร้อยละ 75.3 และผู้ไม่เคยมีประสบการณ์จากผลกระทบขอไวรัสคอมพิวเตอร์ที่ทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เสียหายมีจำนวน 74 นาย คิดเป็นร้อยละ 24.7

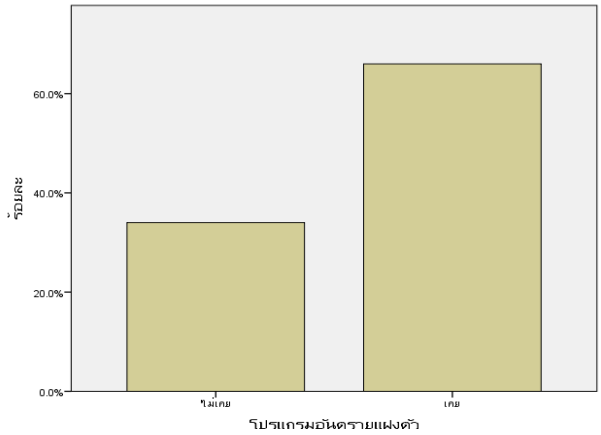
แผนภาพที่ 4-4 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ โดยถูกก่อกวนในระดับเครือข่าย




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากแผนภาพที่ 4-4 แสดงให้เห็นผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากการถูกก่อกวนในระดับเครือข่ายมีจำนวน 191 นาย คิดเป็นร้อยละ 63.7 และผู้ไม่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากการถูกก่อกวนในระดับเครือข่ายมีจำนวน 109 นาย คิดเป็นร้อยละ 36.3

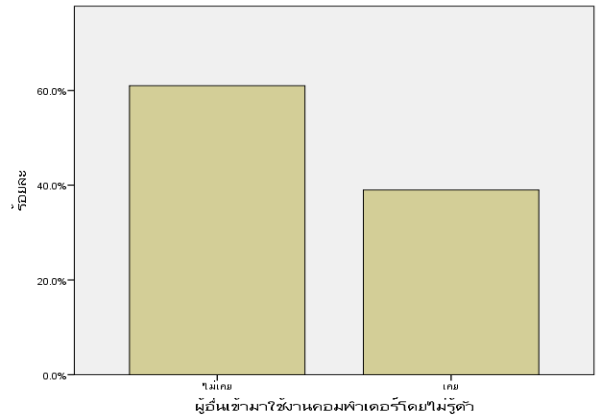
แผนภาพที่ 4-5 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่เคยพบภัยคุกคามทางไซเบอร์ จากโปรแกรมอันตรายที่แฝงตัวเข้ามา




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากแผนภาพที่ 4-5 แสดงผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากโปรแกรมอันตรายที่แฝงตัวเข้ามามีจำนวน 198 นาย คิดเป็นร้อยละ 66 และผู้ไม่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากโปรแกรมอันตรายที่แฝงตัวเข้ามามีจำนวน 102 นาย คิดเป็นร้อยละ 34

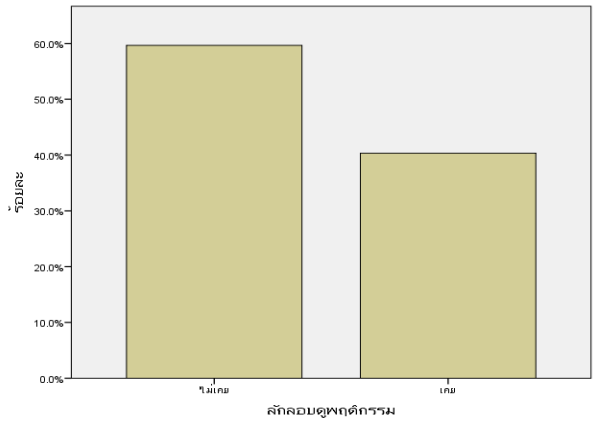
แผนภาพที่ 4-6 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากผู้อื่นเข้ามาใช้งานคอมพิวเตอร์โดยไม่รู้ตัว




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากแผนภาพที่ 4-6 แสดงผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากผู้อื่นเข้ามาใช้งานคอมพิวเตอร์โดยไม่รู้ตัว มีจำนวน 117 นาย คิดเป็นร้อยละ 39 และผู้ไม่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากผู้อื่นเข้ามาใช้งานคอมพิวเตอร์โดยไม่รู้ตัวจำ นวน 183 นาย คิดเป็นร้อยละ 61

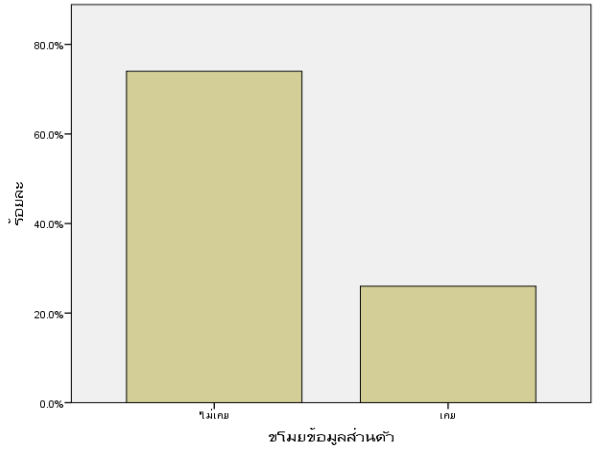
แผนที่ 4-7 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากมีผู้ลักลอบดูพฤติกรรมและบันทึกการใช้งาน




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากแผนภาพที่ 4-7 แสดงผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์จากผู้อื่นลักลอบดูพฤติกรรม และบันทึกการใช้งาน มีจำนวน 65 นาย คิดเป็นร้อยละ 21.7 และผู้ไม่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากการถูกเรียกค่าไถ่ จำนวน 179 นาย คิดเป็นร้อยละ 59.7

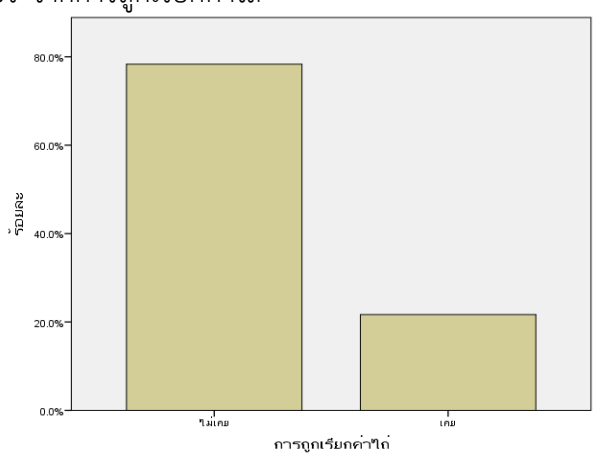
แผนภาพที่ 4-8 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่เคยพบภัยคุกคามทางไซเบอร์ จากการถูกขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากแผนภาพที่ 4-8 แสดงผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากจากการถูกขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน มีจำนวน 65 นาย คิดเป็นร้อยละ 21.7 และผู้ไม่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากการถูกขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงินจำนวน 222 นาย คิดเป็นร้อยละ 74

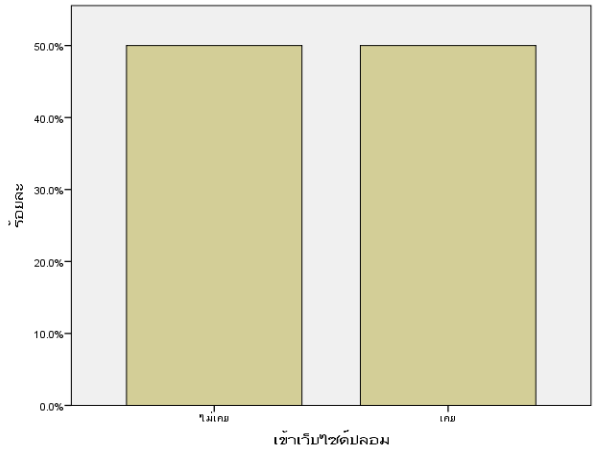
แผนภาพที่ 4-9 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่เคยพบภัยคุกคามทางไซเบอร์ จากการถูกเรียกค่าไถ่




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากแผนภาพที่ 4-9 แสดงผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากการถูกเรียกค่าไถ่ มีจำนวน 65 นาย คิดเป็นร้อยละ 21.7 และผู้ไม่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากการถูกเรียกค่าไถ่ จำนวน 235 คน คิดเป็นร้อยละ 78.3

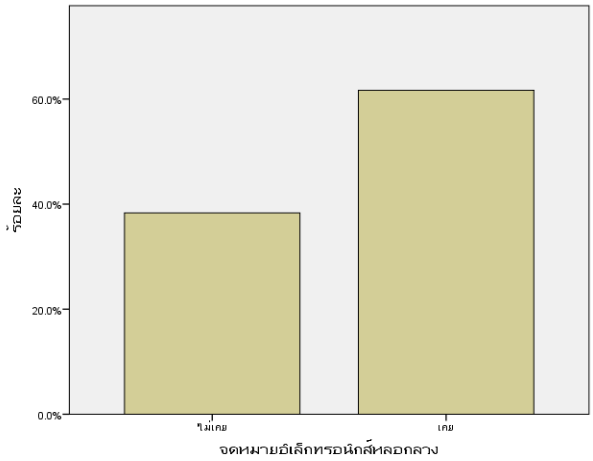
แผนภาพที่ 4-10 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่เคยพบภัยคุกคามทางไซเบอร์ จากการเข้าเว็บไซต์ปลอม




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากแผนภาพที่ 4-10 แสดงผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากการเข้าเว็บไซต์ปลอมมีจำนวน 150 นาย คิดเป็นร้อยละ 50 และผู้ไม่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากการถูกเรียกค่าไถ่ จำนวน 150 นาย คิดเป็นร้อยละ 50

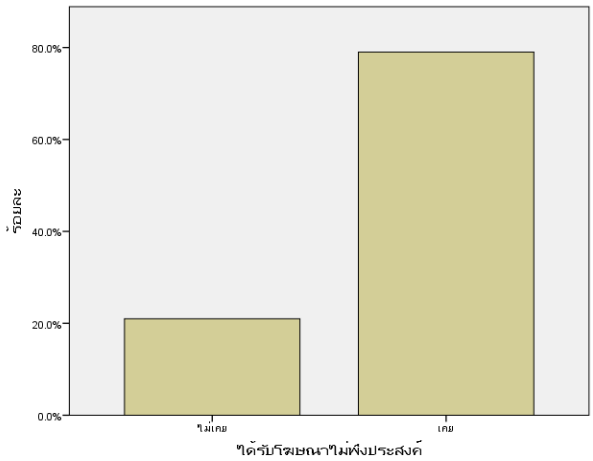
แผนภาพที่ 4-11 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่เคยพบภัยคุกคามทางไซเบอร์ จากจดหมายอิเล็กทรอนิกส์หลอกลวง




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากแผนภาพที่ 4-11 แสดงผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากจดหมายอิเล็กทรอนิกส์ หลอกลวง มีจำนวน 185 นาย คิดเป็นร้อยละ 61.7 และผู้ไม่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากการถูกเรียกค่าไถ่ จำนวน 115 นาย คิดเป็นร้อยละ 38.3

แผนภาพที่ 4-12 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่เคยพบภัยคุกคามทางไซเบอร์ จากโฆษณาไม่พึงประสงค์




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

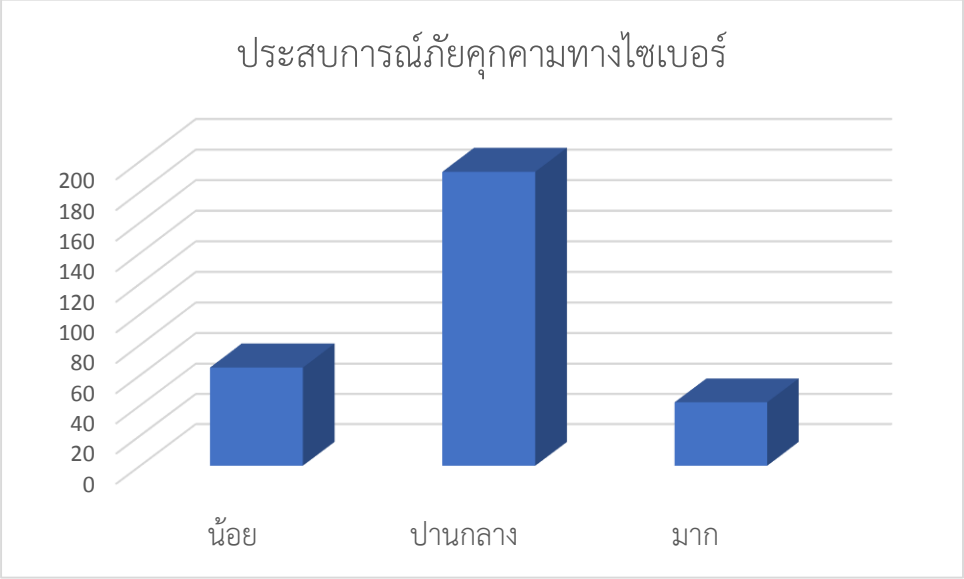
จากแผนภาพที่ 4-12 แสดงผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ จากโฆษณาไม่พึงประสงค์ มีจำนวน 237 นาย คิดเป็นร้อยละ 79 และผู้ไม่มีประสบการณ์ภัยคุกคามทางไซเบอร์จากการถูกเรียกค่าไถ่ จำนวน 63 นาย คิดเป็นร้อยละ 21

ตารางที่ 4-4 แสดงร้อยละของลักษณะทางประชากรของผู้ตอบแบบสอบถามในด้านการจัดกลุ่มระดับประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

| ระดับประสบการณ์ | จำนวน(คน) | ร้อยละ |
|---|---|---|
| น้อย | 65 | 21.7 |
| ปานกลาง | 193 | 64.3 |
| มาก | 42 | 14 |
| **รวม** | 300 | 100 |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

แผนภาพที่ 4-13 แสดงข้อมูลนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปี 2562 ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-4 และแผนภาพที่ 4-13 แสดงผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ โดยแบ่งกลุ่มเป็นผู้มีประสบการณ์น้อย ปานกลาง และมาก โดยผู้ที่มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ส่วนใหญ่จะมีประสบการณ์อยู่ในระดับปานกลางมีจำนวน 193 นาย คิดเป็นร้อยละ 64.3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์น้อยมีจำนวน 65 นาย คิดเป็นร้อยละ 21.7 และนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าที่มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มา

## ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

ตารางที่ 4-5 ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการจารกรรมข้อมูล

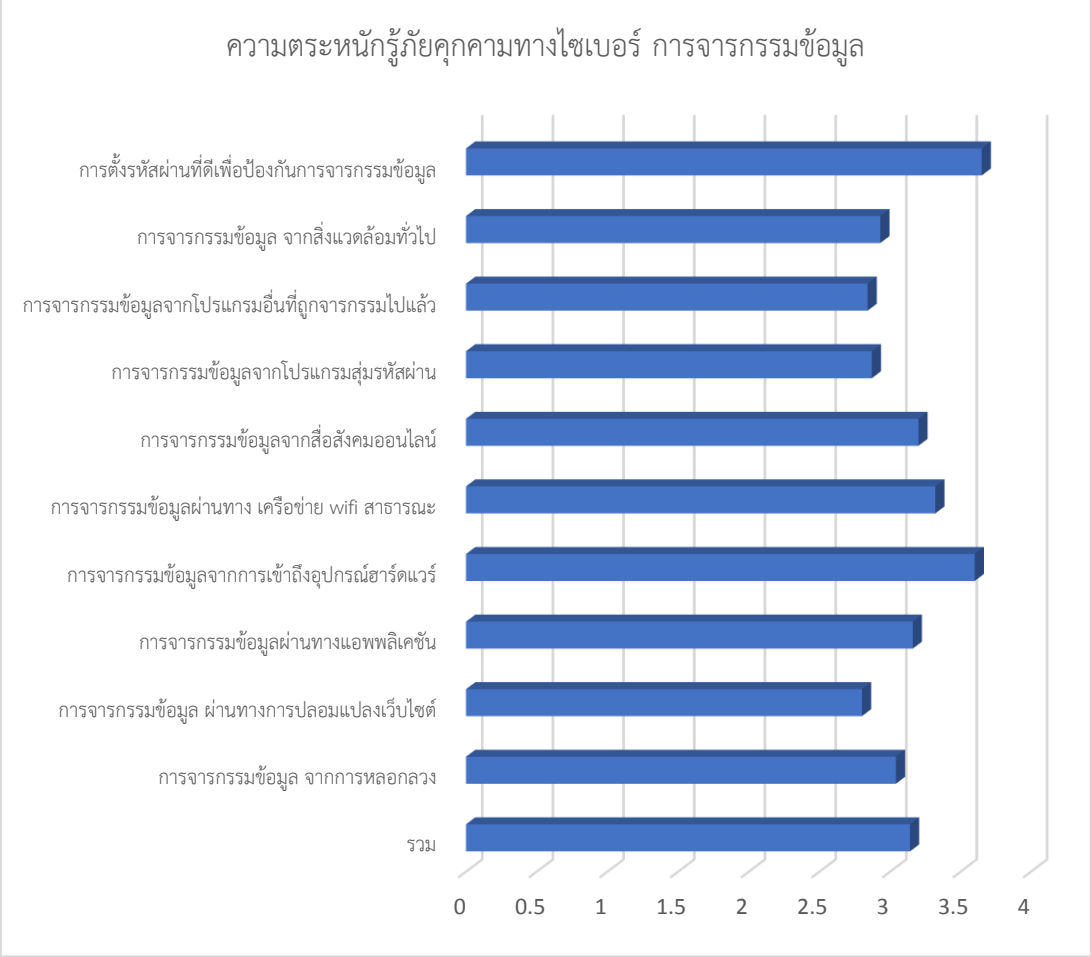
| ความตระหนักรู้ภัยคุกคามทางไซเบอร์ การจารกรรมข้อมูล | | | | |
|---|---|---|---|---|
| เหตุการณ์ | | M | SD | ระดับ |
| 1. | การตั้งรหัสผ่านที่ดีเพื่อป้องกันการจารกรรมข้อมูล<br>คำถาม : นักเรียนตั้งรหัสผ่านมากกว่า 8 ตัวอักษรขึ้นไปหรือไม่ และนักเรียนตั้งรหัสผ่านที่ประกอบด้วยตัวอักษรตัวเล็ก (Lowercase Letter) ตัวใหญ่ (Uppercase Letter) ตัวเลข (Number) และอักษรพิเศษ (Special Letter ต.ย. เช่น @,$,&,฿ เป็นต้น) หรือไม่ | 3.65 | 1.169 | มาก |
| 2. | การป้องกันการจารกรรมข้อมูล จากสิ่งแวดล้อมทั่วไป<br>คำถาม : นักเรียนจดรหัสผ่านไว้ในที่ ๆ นักเรียนสามารถเรียกดูได้หรือไม่ เช่น ในกระดาษหรือในโทรศัพท์มือถือ | 2.93 | 1.281 | ปานกลาง |
| 3. | การป้องกันการจารกรรมข้อมูลจากโปรแกรมอื่นที่ถูกจารกรรมไปแล้ว<br>คำถาม : นักเรียนใช้รหัสผ่านเดียวกันในทุกโปรแกรมหรือไม่ | 2.84 | 1.086 | ปานกลาง |
| 4. | การป้องกันการจารกรรมข้อมูลจากโปรแกรมสุ่มรหัสผ่าน<br>คำถาม : นักเรียนเปลี่ยนรหัสผ่านบ่อยหรือไม่ | 2.87 | 1.090 | ปานกลาง |
| 5. | การป้องกันการจารกรรมข้อมูลจากสื่อสังคมออนไลน์<br>คำถาม : นักเรียนโพสต์ข้อมูลส่วนตัว เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ วันเดือนปีเกิด บนสื่อสังคมออนไลน์หรือไม่ | 3.20 | 1.214 | ปานกลาง |
| 6. | การป้องกันการจารกรรมข้อมูลผ่านทางเครือข่ายสาธารณะ (Free wifi)<br>คำถาม : นักเรียนใช้ Wifi สาธารณะในการเปิดดูข้อมูลส่วนตัว หรือข้อมูลที่มีความสำคัญเช่นข้อมูลทางการเงินหรือไม่ | 3.32 | 1.214 | ปานกลาง |

ตารางที่ 4 - 5...(ต่อ)

| ความตระหนักรู้ภัยคุกคามทางไซเบอร์ การจารกรรมข้อมูล | | | | |
|---|---|---|---|---|
| **เหตุการณ์** | | **M** | **SD** | **ระดับ** |
| 7. | การป้องกันการจารกรรมข้อมูลจากการเข้าถึงอุปกรณ์ฮาร์ดแวร์<br>คำถาม : นักเรียนออกจากระบบ (log out) ทุกครั้งที่ใช้งานโปรแกรมหรือไม่ | 3.60 | 1.256 | มาก |
| 8. | การป้องกันการจารกรรมข้อมูลผ่านทางแอพพลิเคชัน<br>คำถาม : เมื่อเข้าเว็บไซต์ นักเรียนเลือก “Keep me logged in” หรือ “Remember me” หรือไม่ | 3.16 | 1.254 | ปานกลาง |
| 9. | การป้องกันการจารกรรมข้อมูล ผ่านทางการปลอมแปลงเว็บไซต์<br>คำถาม : การทำธุรกรรมทางการเงินบนอินเทอร์เน็ต นักเรียนได้ตรวจสอบ URL ของเว็บไซต์ ว่าเริ่มด้วย https:// หรือไม่ | 2.80 | 1.132 | ปานกลาง |
| 10. | การป้องกันการจารกรรมข้อมูล จากการหลอกลวง<br>คำถาม : หากธนาคารที่นักเรียนใช้บริการอยู่เป็นประจำ ได้ส่งจดหมายอิเล็กทรอนิกส์ (E-mail) มายังนักเรียน เพื่อแจ้งการปรับปรุงระบบรักษาความปลอดภัยระหว่างนักเรียนและธนาคารให้ดียิ่งขึ้น โดยให้นักเรียนเข้าระบบ (Login) ด้วยการกรอกข้อมูลผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อดำเนินการกรอกข้อมูลในการปรับปรุงระบบ นักเรียนจะดำเนินการหรือไม่ | 3.04 | 1.215 | ปานกลาง |
| **รวม** | | **3.14** | **0.423** | **ปานกลาง** |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

แผนภาพที่ 4-14 กราฟแสดงความตระหนักรู้ภัยคุกคามทางไซเบอร์ การจารกรรมข้อมูล




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-5 และแผนภาพที่ 4-14 พบว่าผู้ตอบแบบสอบถาม มีความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการจารกรรมข้อมูลอยู่ในระดับปานกลาง (3.14) โดยการป้องกันการจารกรรมข้อมูลที่กลุ่มตัวอย่างมีความตระหนักมาก คือ การตั้งรหัสผ่านที่ดีเพื่อป้องกันการจารกรรมข้อมูล (3.65) การป้องกันโจรกรรมข้อมูลจากการเข้าถึงอุปกรณ์ฮาร์ดแวร์ (3.60) ส่วนกลุ่มตัวอย่างมีความตระหนักในระดับปานกลาง คือ การป้องกันการจารกรรมข้อมูลผ่านทางเครือข่ายสาธารณะ (Free Wifi) (3.32) การป้องกันการจารกรรมข้อมูลจากสื่อสังคมออนไลน์ (3.20) การป้องกันการจารกรรมข้อมูลผ่านทางแอพพลิเคชัน (3.16) การป้องกันการจารกรรมข้อมูลจากการหลอกลวง (3.04) การป้องกันการจารกรรมข้อมูล จากสิ่งแวดล้อมทั่วไป (2.93) การป้องกันการจารกรรมข้อมูลจากโปรแกรมสุ่มรหัสผ่าน (2.87) การป้องกันการจารกรรมข้อมูล ผ่านทางการปลอมแปลงเว็บไซต์ (2.80)

ตารางที่ 4-6 ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้าย

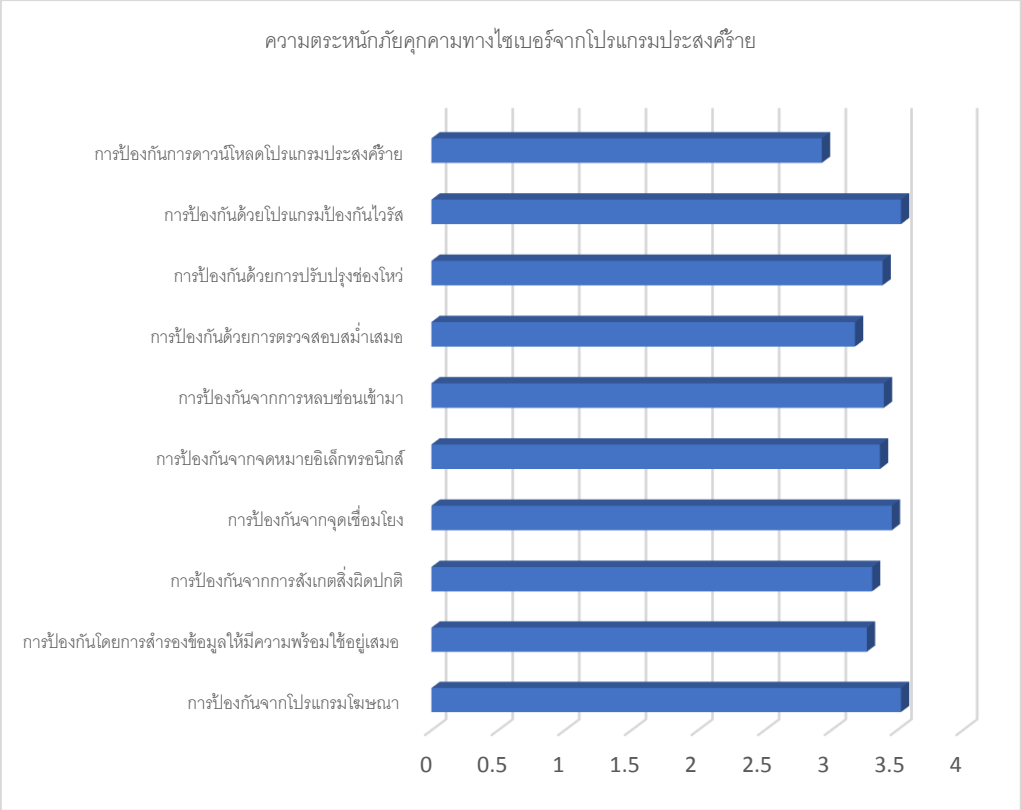
| ประเด็นความตระหนักรู้ภัยคุกคามทางไซเบอร์ การโปรแกรมประสงค์ร้าย | | | | |
|---|---|---|---|---|
| **ลำดับ** | **เหตุการณ์** | M | SD | **ระดับ** |
| 1. | การป้องกันการดาวน์โหลดโปรแกรมประสงค์ร้าย (Malicious Software)<br>คำถาม : นักเรียนจะดาวน์โหลดโปรแกรมฟรีบนอินเทอร์เน็ตมาติดตั้งบนเครื่องคอมพิวเตอร์ | 2.93 | 1.175 | ปานกลาง |
| 2. | การป้องกันโปรแกรมประสงค์ร้ายด้วยโปรแกรมป้องกันไวรัส (Anti-Virus)<br>คำถาม : นักเรียนติดตั้งโปรแกรมป้องกันไวรัสที่ระบบคอมพิวเตอร์หรือไม่ | 3.53 | 1.055 | มาก |
| 3. | การป้องกันโปรแกรมประสงค์ร้ายจากการปรับปรุงช่องโหว่ (update patch)<br>คำถาม : นักเรียนอัพเดตโปรแกรม,แอพพลิเคชัน อย่างสม่ำเสมอหรือไม่ | 3.39 | 0.986 | ปานกลาง |
| 4. | การป้องกันโปรแกรมประสงค์ร้ายจากการตรวจสอบสม่ำเสมอ<br>คำถาม : ก่อนใช้งานอุปกรณ์สำรองข้อมูลนักเรียนทำการสแกนไวรัสทุกครั้งหรือไม่ | 3.18 | 1.076 | ปานกลาง |
| 5. | การป้องกันโปรแกรมประสงค์ร้ายจากการหลบซ่อนเข้ามา (Trojan Horse)<br>คำถาม : หากนักเรียนบังเอิญพบอุปกรณ์อิเล็กทรอนิกส์เช่น ทรัมป์ไดรฟ์ หรือ External Hard Disk ซึ่งไม่ทราบว่าเป็นของผู้ใด นักเรียนจะนำอุปกรณ์เหล่านี้ไปเปิดดูบนเครื่องคอมพิวเตอร์หรือไม่ | 3.40 | 1.253 | ปานกลาง |
| 6. | การป้องกันโปรแกรมประสงค์ร้ายมาจากจดหมายอิเล็กทรอนิกส์ (e-mail)<br>คำถาม : นักเรียนเปิดไฟล์แนบ (Attachment) ในจดหมายอิเล็กทรอนิกส์ (email) จากผู้ที่ไม่รู้จัก หรือไม่ทราบแหล่งที่มาหรือไม่ | 3.37 | 1.168 | ปานกลาง |

ตารางที่ 4 - 6...(ต่อ)

| ประเด็นความตระหนักรู้ภัยคุกคามทางไซเบอร์ การโปรแกรมประสงค์ร้าย | | | | |
|---|---|---|---|---|
| **ลำดับ** | **เหตุการณ์** | M | SD | **ระดับ** |
| 7. | การป้องกันโปรแกรมประสงค์ร้ายจากจุดเชื่อมโยง (Link)<br>คำถาม : นักเรียนคลิกไปยังลิงค์ (Link) ของผู้ไม่รู้จักหรือไม่รู้จักแหล่งที่มาหรือไม่ | 3.46 | 1.073 | ปานกลาง |
| 8. | การป้องกันโปรแกรมประสงค์ร้ายจากการสังเกตสิ่งผิดปกติ<br>คำถาม : นักเรียนสังเกตการทำงานของเครื่องคอมพิวเตอร์เสมอ เช่น การทำงานที่ช้าลง การรับ-ส่งข้อมูลที่ช้าลง และตรวจสอบว่ามีความผิดปกติหรือไม่ | 3.31 | 1.073 | ปานกลาง |
| 9. | การป้องกันโปรแกรมประสงค์ร้ายโดยการสำรองข้อมูลให้มีความพร้อมใช้อยู่เสมอ (Availability)<br>คำถาม : นักเรียนมีการสำรองข้อมูลสำคัญให้พอเพียงพร้อมใช้งานอยู่เสมอหรือไม่ | 3.27 | 0.984 | ปานกลาง |
| 10. | การป้องกันโปรแกรมประสงค์ร้ายจาก Adware<br>คำถาม : นักเรียนกดดู โฆษณา เมื่อขึ้นมาบนจอคอมพิวเตอร์ (Pop-up Ads) หรือไม่ | 3.53 | 1.225 | มาก |
| **รวม** | | **3.337** | **0.530** | |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

แผนภาพที่ 4-15 กราฟแสดงความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้าย




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-6 และ แผนภาพที่ 4-15 ผู้ตอบแบบสอบถาม มีความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้ายอยู่ในระดับปานกลาง (3.33) โดยการป้องกันโปรแกรมประสงค์ร้ายที่กลุ่มตัวอย่างมีความตระหนักมาก คือ การป้องกันตนเองด้วยโปรแกรมป้องกันไวรัส (3.53) และการป้องกันตนเองจากโปรแกรมโฆษณา (3.53) กลุ่มตัวอย่างมีความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้ายในระดับปานกลาง คือ การป้องกันโปรแกรมประสงค์ร้ายจากจุดเชื่อมโยง (Link) (3.46) การป้องกันโปรแกรมประสงค์ร้ายจากการหลบซ่อนเข้ามา (Trojan Horse) (3.40) การป้องกันโปรแกรมประสงค์ร้ายจากการปรับปรุงช่องโหว่ (Update patch) (3.39) การป้องกันโปรแกรมประสงค์ร้ายมาจากจดหมายอิเล็กทรอนิกส์ (e-mail) (3.37) การป้องกันโปรแกรมประสงค์ร้ายจากการตรวจสอบสม่ำเสมอ (3.31) การป้องกันโปรแกรมประสงค์ร้ายจากการสังเกตสิ่งผิดปกติ (3.31) การป้องกันโปรแกรมประสงค์ร้ายโดยการสำรองข้อมูลให้มีความพร้อมใช้อยู่เสมอ (3.27) การป้องกันโปรแกรมประสงค์ร้ายจากการตรวจสอบสม่ำเสมอ (3.18) การป้องกันการดาวน์โหลดโปรแกรมประสงค์ร้าย (Malicious Software) (2.93)

ตารางที่ 4-7 ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม

| ความตระหนักรู้ภัยคุกคามทางไซเบอร์ จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม | | | | |
|---|---|---|---|---|
| **ลำดับ** | **เหตุการณ์** | M | SD | **ระดับ** |
| 1. | การไม่แชร์ข้อมูลที่ไม่ถูกต้อง ทางสื่อสังคมออนไลน์<br>คำถาม : เมื่อได้รับจดหมายลูกโซ่ หรือข้อมูลข่าวสาร นักเรียนส่งต่อหรือทำการแชร์ข้อมูลโดยไม่มีการตรวจสอบความถูกต้องหรือไม่ | 3.71 | 1.245 | มาก |
| 2. | การไม่หลงเชื่อข้อมูลที่ไม่ถูกต้อง ทางสื่อสังคมออนไลน์<br>คำถาม : หากนักเรียนเชื่อหรือปฏิบัติตามข้อมูลบนสื่อออนไลน์ นักเรียนได้ทำการหาข้อมูล วิเคราะห์ และสรุปผลหาความถูกต้องก่อนที่จะเชื่อหรือปฏิบัติตามหรือไม่ | 3.40 | 3.109 | ปานกลาง |
| 3. | การไม่แอบอ้าง ทางสื่อสังคมออนไลน์ (Non-Masquerading)<br>คำถาม : นักเรียนนำภาพหรือข้อมูลของผู้อื่นที่ได้จากการคัดลอก (copy) หรือ ดาวน์โหลด (Download) โดยไม่ได้รับอนุญาตมาโพสต์ โดยไม่ได้ให้เครดิตเจ้าของภาพหรือไม่ | 3.42 | 1.144 | ปานกลาง |
| 4. | การไม่ทำให้ผู้อื่นอับอายหรือเสียชื่อเสียง ทางสื่อสังคมออนไลน์<br>คำถาม : นักเรียนเคยกล่าวถึงผู้อื่นให้ได้รับความอับอายเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์หรือไม่ | 3.74 | 1.197 | มาก |
| 5. | การไม่ใช้ข้อความหยาบคาย ด่าว่าผู้อื่น ทางสื่อสังคมออนไลน์ (Non-Flamming)<br>คำถาม : นักเรียนเคยกล่าวถึงผู้อื่นให้ได้รับความอับอายเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์หรือไม่ | 3.54 | 1.194 | มาก |
| 6. | การไม่ล้อเลียนรูปร่างหน้าตาของผู้อื่นทางสื่อสังคมออนไลน์<br>คำถาม : นักเรียนเคยล้อเลียนรูปร่างหน้าตาของผู้อื่นผ่านทางไซเบอร์หรือไม่ | 3.74 | 1.207 | มาก |
| 7. | การไม่เผยแพร่ข่าวลือในทางลบของผู้อื่นทางสื่อสังคมออนไลน์<br>คำถาม : นักเรียนเคยเผยแพร่ข่าวลือในทางลบของผู้อื่นผ่านทางไซเบอร์หรือไม่ | 3.78 | 1.190 | มาก |

ตารางที่ 4 – 7...(ต่อ)

| ความตระหนักรู้ภัยคุกคามทางไซเบอร์ จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม | | | | |
|---|---|---|---|---|
| **ลำดับ** | **เหตุการณ์** | M | SD | **ระดับ** |
| 8. | การไม่เผยแพร่ข้อมูลส่วนบุคคลของผู้อื่นทางสื่อสังคมออนไลน์ (Non-Outing)<br>คำถาม : นักเรียนเคยนำข้อมูลส่วนบุคคลของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์หรือไม่ | 3.78 | 1.232 | มาก |
| 9. | การเคารพสิทธิของผู้อื่นทางสื่อสังคมออนไลน์ (Respect)<br>คำถาม : นักเรียนเคยลบรายชื่อบุคคลที่ไม่ชอบออกจากลุ่มสนทนาทางไซเบอร์หรือไม่ | 3.29 | 1.197 | ปานกลาง |
| 10. | การไม่กีดกันผู้อื่นทางสื่อสังคมออนไลน์ (Non-Exclusion)<br>คำถาม : นักเรียนเคยกดดันให้บุคคลที่ไม่ชอบให้ออกจากกลุ่มสนทนาทางไซเบอร์หรือไม่ | 3.70 | 1.250 | มาก |
| **รวม** | | **3.607** | **0.816** | |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

แผนภาพที่ 4-16 กราฟแสดงความตระหนักรู้ภัยคุกคามทางไซเบอร์จากจากการใช้สื่อสังคมออนไลน์ที่ไม่ภาพเหมาะสม


ที่มา : ประมวลผลโดยผู้วิจัย , 2563

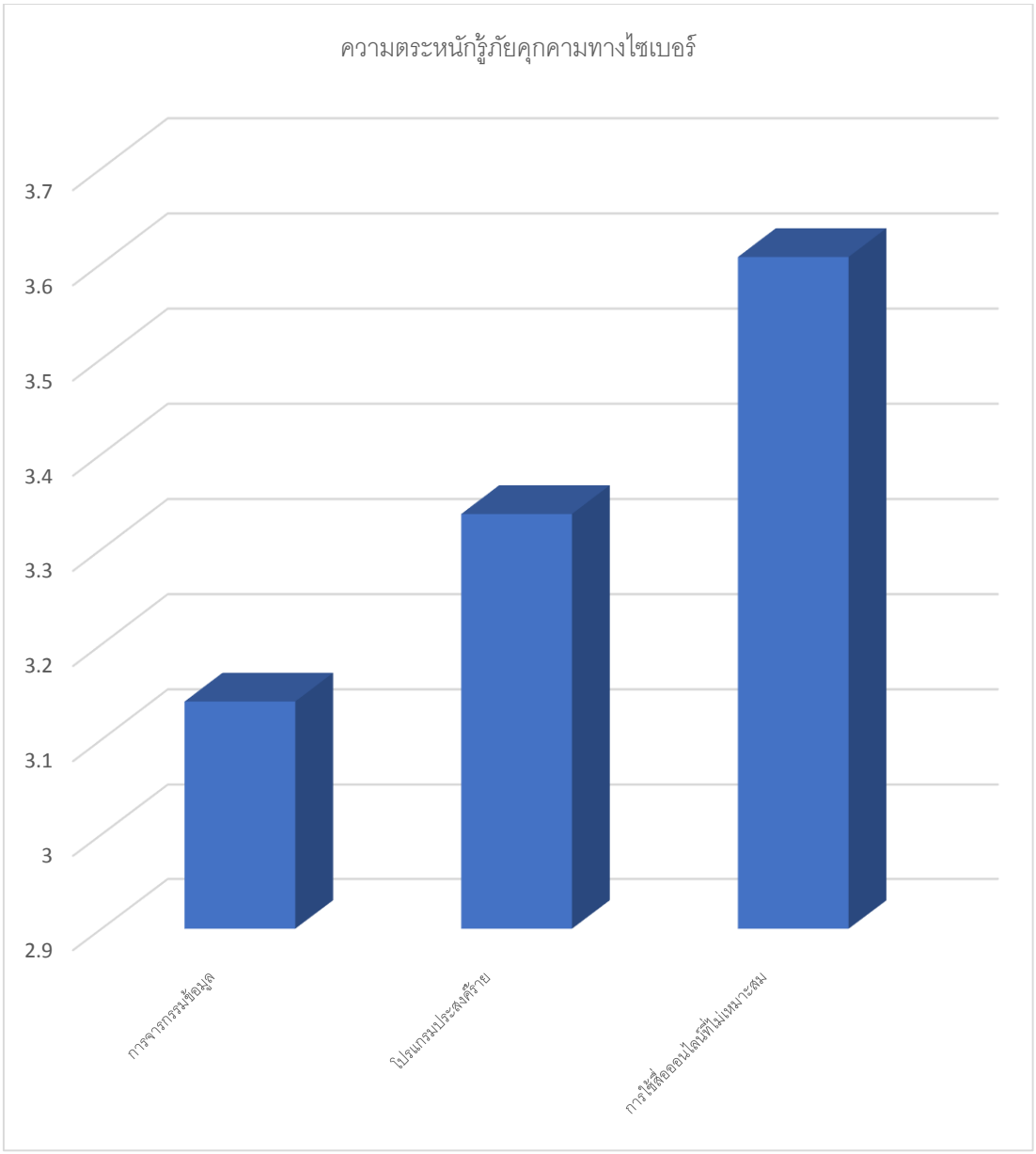
จากตารางที่ 4-7 และแผนภาพที่ 14-6 พบว่าผู้ตอบแบบสอบถาม มีความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสมอยู่ในระดับสูง (3.60) โดยการใช้สื่อสังคมออนไลน์ที่กลุ่มตัวอย่างมีความตระหนักมาก คือ การไม่เผยแพร่ข่าวลือในทางลบของผู้อื่นทางสื่อสังคมออนไลน์ (3.78) และการไม่เผยแพร่ข้อมูลส่วนบุคคลของผู้อื่นทางสื่อสังคมออนไลน์ (Non-Outing) (3.78) การไม่ทำให้ผู้อื่นอับอายหรือเสียชื่อเสียง ทางสื่อสังคมออนไลน์ (Non-Harassment) (3.74) การไม่ล้อเลียนรูปร่างหน้าตาของผู้อื่นทางสื่อสังคมออนไลน์ (Non-Harassment) (3.74) การไม่แชร์ข้อมูลที่ไม่ถูกต้อง ทางสื่อสังคมออนไลน์ (3.71) การไม่กีดกันผู้อื่นทางสื่อสังคมออนไลน์ (Non-Exclusion) (3.70) การไม่ใช้ข้อความหยาบคายด่าว่าผู้อื่น ทางสื่อสังคมออนไลน์ (Non-Flamming) (3.54) ความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสมอยู่ในระดับปานกลาง คือ การไม่แอบอ้าง ทางสื่อสังคมออนไลน์ (Non-Masquerading) (3.42) การไม่หลงเชื่อข้อมูลที่ไม่ถูกต้อง ทางสื่อสังคมออนไลน์ (3.40) และการเคารพสิทธิของผู้อื่นทางสื่อสังคมออนไลน์ (Respect) (3.29)

ตารางที่ 4-8 ค่าเฉลี่ยและค่าเบี่ยงเบนมาตรฐานของความตระหนักรู้ภัยคุกคามทางไซเบอร์ทุกด้าน (การจารกรรมข้อมูล , โปรแกรมประสงค์ร้าย , การใช้สื่อออนไลน์ที่ไม่เหมาะสม)

| ความตระหนักรู้ภัยคุกคามทางไซเบอร์ | | | | | | |
|---|---|---|---|---|---|---|
| ประเด็น | N | Min | Max | M | SD | ระดับ |
| การจารกรรมข้อมูล | 300 | 2.00 | 4.50 | 3.140 | 0.423 | ปานกลาง |
| โปรแกรมประสงค์ร้าย | 300 | 2.20 | 5.00 | 3.337 | 0.530 | ปานกลาง |
| การใช้สื่อออนไลน์ที่ไม่เหมาะสม | 300 | 1.80 | 5.00 | 3.607 | 0.795 | มาก |
| รวม | 300 | 2.40 | 4.83 | 3.361 | 0.469 | ปานกลาง |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

แผนภาพที่ 4-17 กราฟแสดงความตระหนักรู้ภัยคุกคามทางไซเบอร์




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-8 และแผนภาพที่ 4-17 พบว่า ผู้ตอบแบบสอบถามมีความตระหนักรู้ภัยคุกคามทางไซเบอร์การใช้สื่อออนไลน์ที่ไม่เหมาะสมอยู่ในระดับสูง (3.607) รองลงมาคือความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้ายระดับปานกลาง (3.337) และความตระหนักรู้ภัยคุกคามทางไซเบอร์ด้านการจารกรรมข้อมูลระดับปานกลาง (3.14)

## การทดสอบสมมติฐาน

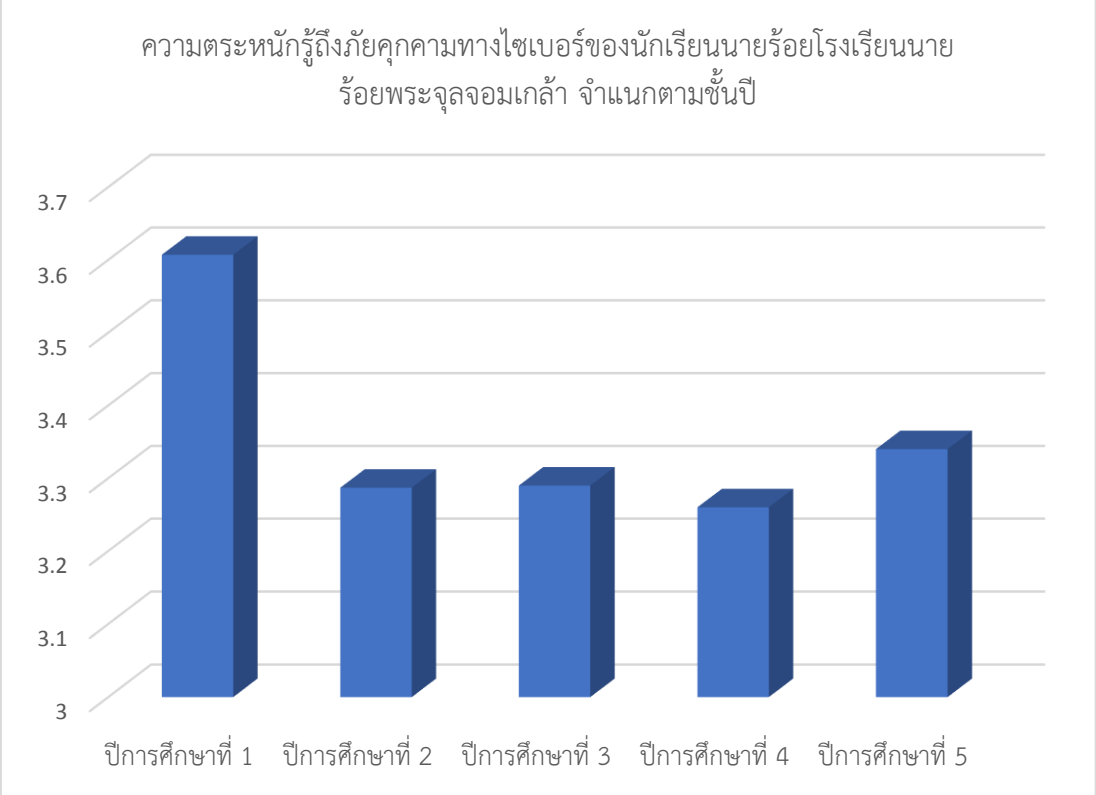
**1. ปัจจัยทางด้านชั้นปีการศึกษามีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า**

ตารางที่ 4-9 การเปรียบเทียบความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามชั้นปี

| ชั้นปีการศึกษา | N | M | SD | ระดับ |
|---|---|---|---|---|
| ปีการศึกษาที่ 1 | 63 | 3.607 | 0.548 | มาก |
| ปีการศึกษาที่ 2 | 55 | 3.287 | 0.399 | ปานกลาง |
| ปีการศึกษาที่ 3 | 61 | 3.292 | 0.466 | ปานกลาง |
| ปีการศึกษาที่ 4 | 60 | 3.262 | 0.474 | ปานกลาง |
| ปีการศึกษาที่ 5 | 61 | 3.340 | 0.350 | ปานกลาง |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

ภาพที่ 4-18 กราฟแสดงความตระหนักรู้ภัยคุกคามทางไซเบอร์จำแนกตามชั้นปี




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-9 และแผนภาพที่ 4-18 พบว่า ผู้ตอบแบบสอบถามมีความตระหนักรู้ภัยคุกคามทางไซเบอร์แยกตามชั้นปี พบว่า นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 1 มีความตระหนักรู้ในระดับสูง มีค่าเฉลี่ยมากที่สุด (3.607) รองลงมาคือนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 5 (3.340) นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 3 (3.292) นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 2 (3.287) และ นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 4 (3.262)

ตารางที่ 4-10 การวิเคราะห์ความแปรปรวนแบบทางเดียวของความตระหนักภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามชั้นปี

| **ความตระหนัก** | **แหล่งที่มา** | **SS** | **df** | **MS** | **F** | **P** |
|---|---|---|---|---|---|---|
| การโจรกรรมข้อมูล | ระหว่างกลุ่ม | 1.077 | 4 | .269 | 1.511 | .199 |
| | ภายในกลุ่ม | 52.585 | 295 | .178 | | |
| | รวม | 53.662 | 299 | | | |
| โปรแกรมประสงค์ร้าย | ระหว่างกลุ่ม | 8.952 | 4 | 2.238 | 8.783*** | .000 |
| | ภายในกลุ่ม | 75.170 | 295 | .255 | | |
| | รวม | 84.122 | 299 | | | |
| สื่อออนไลน์ไม่เหมาะสม | ระหว่างกลุ่ม | 5.370 | 4 | 1.342 | 6.775*** | .000 |
| | ภายในกลุ่ม | 58.456 | 295 | .198 | | |
| | รวม | 63.825 | 299 | | | |
| รวม | ระหว่างกลุ่ม | 5.012 | 4 | 1.253 | 6.063*** | .000 |
| | ภายในกลุ่ม | 60.963 | 295 | .207 | | |
| | รวม | 65.974 | 299 | | | |

หมายเหตุ *** มีนัยสำคัญทางสถิติที่ระดับ 0.05

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-10 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ ชั้นปีการศึกษามีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าที่ระดับนัยสำคัญ 0.05 ($p<0.05$)

ตารางที่ 4-11 การเปรียบเทียบความแตกต่างระหว่างความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามชั้นปีการศึกษา

| **ชั้นปีการศึกษา** | | **ความแตกต่างของค่าเฉลี่ย** | **P** |
|---|---|---|---|
| ชั้นปีที่ 1 | ชั้นปีที่ 2 | .32469* | .000 |
| | ชั้นปีที่ 3 | .31451* | .000 |
| | ชั้นปีที่ 4 | .34463* | .000 |
| | ชั้นปีที่ 5 | .26697* | .000 |
| ชั้นปีที่ 2 | ชั้นปีที่ 1 | -.32469* | .000 |
| | ชั้นปีที่ 3 | -.01018 | .905 |
| | ชั้นปีที่ 4 | .01994 | .816 |
| | ชั้นปีที่ 5 | -.05772 | .498 |
| ชั้นปีที่ 3 | ชั้นปีที่ 1 | -.31451* | .000 |
| | ชั้นปีที่ 2 | .01018 | .905 |
| | ชั้นปีที่ 4 | -.04754 | .716 |
| | ชั้นปีที่ 5 | -.04757 | .564 |
| ชั้นปีที่ 4 | ชั้นปีที่ 1 | -.34463* | .000 |
| | ชั้นปีที่ 2 | -.01994 | .816 |
| | ชั้นปีที่ 3 | -.03012 | .716 |
| | ชั้นปีที่ 5 | -.07766 | .349 |
| ชั้นปีที่ 5 | ชั้นปีที่ 1 | -.26697* | .001 |
| | ชั้นปีที่ 2 | .05772 | .498 |
| | ชั้นปีที่ 3 | .04754 | .564 |
| | ชั้นปีที่ 4 | .07766 | .349 |

หมายเหตุ *** มีนัยสำคัญทางสถิติที่ระดับ 0.05

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-11 พบว่า นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 1 จะมีความตระหนักรู้ภัยคุกคามทางไซเบอร์มากกว่าชั้นปีที่ 2 ชั้นปีที่ 3 ชั้นปีที่ 4 และ ชั้นปีที่ 5 อย่างมีนัยสำคัญ

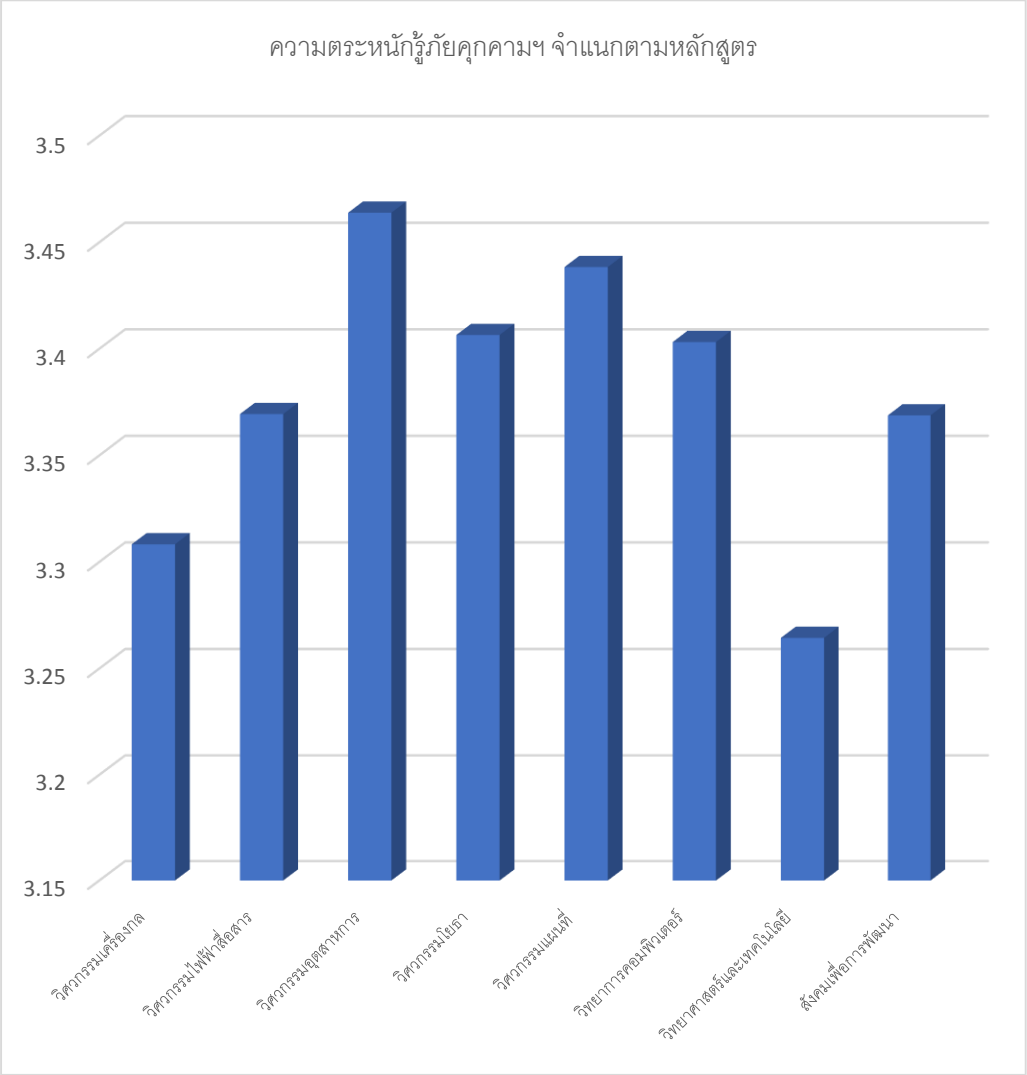
**2. ปัจจัยด้านหลักสูตรการศึกษามีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า**

ตารางที่ 4-12 การเปรียบเทียบความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามหลักสูตรการศึกษา

| หลักสูตร | N | M | SD |
|---|---|---|---|
| วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล | 20 | 3.3083 | .35834 |
| วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร | 24 | 3.3694 | .52686 |
| วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมอุตสาหการ | 24 | 3.4639 | .58927 |
| วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมโยธา | 31 | 3.4065 | .45153 |
| วิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมแผนที่ | 33 | 3.43838 | .44293 |
| วิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ | 31 | 3.4032 | .45537 |
| วิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี | 59 | 3.2644 | .46530 |
| ศิลปศาสตรบัณฑิต สาขาวิชาสังคมเพื่อการพัฒนา | 77 | 3.3688 | .47238 |

ทีมา : ประมวลผลโดยผู้วิจัย , 2563

แผนภาพที่ 4-19 กราฟแสดงความตระหนักรู้ภัยคุกคามทางไซเบอร์จำแนกตามหลักสูตร




ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-12 และแผนภาพที่ 4-19 พบว่า ผู้ตอบแบบสอบถามมีความตระหนักรู้ภัยคุกคามทางไซเบอร์แยกตามหลักสูตร พบว่า นักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้ามีความตระหนักรู้ในระดับปานกลาง โดยหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมอุตสาหการมีความตระหนักมากที่สุด (3.46) หลักสูตรที่มีความตระหนักรู้ภัยคุกคามทางไซเบอร์ รองลงมาคือ หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมแผนที่ (3.43) หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมโยธา (3.406) หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ (3.403) หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร (3.369) ศิลปศาสตรบัณฑิต สาขาวิชาสังคมเพื่อการพัฒนา (3.368) วิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล (3.308) และหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี (3.264) ตามลำดับ

ตารางที่ 4-13 การวิเคราะห์ความแปรปรวนแบบทางเดียวของการตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามหลักสูตรการศึกษา

| **แหล่งที่มา** | SS | Df | MS | F | P |
|---|---|---|---|---|---|
| ระหว่างกลุ่ม | 1.003 | 7 | .143 | .642 | .721 |
| ภายในกลุ่ม | 64.942 | 291 | .223 | | |
| รวม | 65.945 | 298 | | | |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-13 พบว่า ปฏิเสธสมมติฐานการวิจัย กล่าวคือ หลักสูตรการศึกษาไม่มีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ที่ระดับนัยสำคัญ 0.05 ($p<0.05$)

ตารางที่ 4-14 การเปรียบเทียบความแตกต่างระหว่างความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามหลักสูตรการศึกษา

| **หลักสูตร** | | **ความแตกต่างของค่าเฉลี่ย** | **p** |
|---|---|---|---|
| - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร | -.06111 | |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ | -.15556 | |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา | -.09812 | |
| | - หลักสูตรวิศวกรรมบัณฑิต สาขาวิชาวิศวกรรมแผนที่ | -.075510 | |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ | -.09489 | |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี | .03944 | |
| | - หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา | -.06050 | |
| - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล | .06111 | |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ | -.09444 | |

ตารางที่ 4 – 14...(ต่อ)

| หลักสูตร | | ความแตกต่างของค่าเฉลี่ย | p |
|---|---|---|---|
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา | -.03701 | |
| | - หลักสูตรวิศวกรรมบัณฑิต สาขาวิชาวิศวกรรมแผนที่ | -.01439 | |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ | -.03378 | |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี | .10056 | |
| | - หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา | .00061 | |
| - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล | .15556 | |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร | .09444 | |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา | .57444 | |
| | - หลักสูตรวิศวกรรมบัณฑิต สาขาวิชาวิศวกรรมแผนที่ | .08005 | |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ | .06066 | |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี | .19500 | .669 |
| | - หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา | .09506 | .277 |
| - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล | .09812 | .469 |

ตารางที่ 4 – 14...(ต่อ)

| หลักสูตร | | ความแตกต่างของค่าเฉลี่ย | p |
|---|---|---|---|
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร | .03701 | .573 |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ | -.05744 | .484 |
| | - หลักสูตรวิศวกรรมบัณฑิต สาขาวิชาวิศวกรรมแผนที่ | .02261 | .746 |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ | .00323 | .610 |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี | .13756 | .669 |
| | - หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา | .03762 | .489 |
| - หลักสูตรวิศวกรรมบัณฑิต สาขาวิชาวิศวกรรมแผนที่ | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล | .07551 | .773 |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร | .01439 | .910 |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ | -.08005 | .792 |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา | -.02261 | .378 |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ | -.01939 | .996 |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี | .11495 | .277 |
| | - หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา | .01501 | .489 |
| -หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล | .09489 | .655 |

ตารางที่ 4 – 14...(ต่อ)

| หลักสูตร | | ความแตกต่างของค่าเฉลี่ย | p |
|---|---|---|---|
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร | .03378 | .528 |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ | -.06066 | .63 |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา | -.00323 | .088 |
| | - หลักสูตรวิศวกรรมบัณฑิต สาขาวิชาวิศวกรรมแผนที่ | .01939 | .390 |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี | .13434 | .469 |
| | - หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา | -.09994 | .773 |
| -หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล | .06050 | .655 |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร | -.00061 | .848 |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ | -.09506 | .979 |
| | - หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา | -.03762 | .789 |
| | - หลักสูตรวิศวกรรมบัณฑิต สาขาวิชาวิศวกรรมแผนที่ | -.01501 | .708 |
| | - หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ | -.03439 | .528 |
| | - หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา | .09994 | .910 |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-14 พบว่า นักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าในแต่ละหลักสูตร จะมีความตระหนักรู้ภัยคุกคามทางไซเบอร์อยู่ในระดับปานกลาง ไม่แตกต่างกัน

**3. ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า**

ตารางที่ 4-15 การเปรียบเทียบความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามความตระหนักรู้ภัยคุกคามทางไซเบอร์

| ประสบการณ์ | Mean | N | SD. | ระดับ |
|---|---|---|---|---|
| น้อย | 3.5010 | 65 | .54661 | มาก |
| ปานกลาง | 3.3337 | 193 | .46450 | ปานกลาง |
| มาก | 3.2738 | 42 | .29991 | ปานกลาง |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

ตารางที่ 4-16 การวิเคราะห์ความแปรปรวนแบบทางเดียวของการตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามประสบการณ์ภัยคุกคามทางไซเบอร์

| แหล่งที่มา | SS | df | MS | F | P |
|---|---|---|---|---|---|
| ระหว่างกลุ่ม | 1.738 | 2 | 0869 | 4.017* | .019 |
| ภายในกลุ่ม | 64.237 | 297 | .216 | | |
| รวม | 65.974 | 299 | | | |

หมายเหตุ *** มีนัยสำคัญทางสถิติที่ระดับ 0.05

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-16 พบว่า ยอมรับสมมติฐานการวิจัย กล่าวคือ ประสบการณ์ภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าที่ระดับนัยสำคัญ 0.05 ($p<0.05$)

ตารางที่ 4-17 การเปรียบเทียบความแตกต่างระหว่างความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามประสบการณ์ภัยคุกคามทางไซเบอร์

| **ประสบการณ์ภัยคุกคามทางไซเบอร์** | | **ความแตกต่างของค่าเฉลี่ย** | **P** |
|---|---|---|---|
| ประสบการณ์น้อย | ประสบการณ์ปานกลาง<br>ประสบการณ์มาก | .16735*<br>.022722* | .013<br>.014 |
| ประสบการณ์ปานกลาง | ประสบการณ์น้อย<br>ประสบการณ์มาก | -.16735*<br>.05987 | .013<br>.450 |
| ประสบการณ์มาก | ประสบการณ์น้อย<br>ประสบการณ์ปานกลาง | -.022722*<br>-.05987 | .014<br>.450 |

หมายเหตุ *** มีนัยสำคัญทางสถิติที่ระดับ 0.05

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

จากตารางที่ 4-17 พบว่า นักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าที่มีประสบการณ์ภัยคุกคามทางไซเบอร์น้อย จะมีความตระหนักรู้ภัยคุกคามทางไซเบอร์มากกว่านักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ระดับปานกลาง และระดับสูง อย่างมีนัยสำคัญ

## แนวความคิดเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

ตารางที่ 4-18 แนวความคิดเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

| ลำดับ | ภัยคุกคามทางไซเบอร์ | ความคิดเห็นของผู้ให้สัมภาษณ์ | ข้อเสนอแนะของผู้ให้สัมภาษณ์ |
|---|---|---|---|
| 1 | เนื้อหาที่เป็นภัยคุกคม | - ขาดความยั้งคิดก่อนที่จะทำสิ่งต่าง ๆ บนสื่อสังคมออนไลน์<br>-สื่อที่ไม่เหมาะสม เช่นเว็บไซต์พนัน | - จึงควรมีความระมัดระวังในการใช้สื่อคิดและวิเคราะห์ให้ดีก่อนที่จะเผยแพร่<br>- ควรมีการบล็อคเว็บไซต์ที่ไม่เหมาะสม |
| | การโจมตีสภาพความพร้อมใช้ของระบบ | - อาจมีการโจมตีระบบเครือข่าย | - ควรมีการกำหนดมาตรการใช้อินเทอร์เน็ตในองค์กร<br>- มีอุปกรณ์ป้องกันระบบเครือข่าย ทำหน้าที่เป็นตัวกรองข้อมูลภายในองค์กรเพื่อความปลอดภัยของข้อมูล<br>- ผู้ดูแลระบบต้องอัพเดทอุปกรณ์และแอพพลิเคชั่นอยู่เสมอ<br>- ผู้ดูแลระบบต้อง Monitor ดู Log file ว่ามีการเข้าออกข้อมูลอย่างผิดปกติอย่างไรเพื่อทำการแก้ไขได้อย่างทันท่วงที<br>- ห้ามบุคคลภายนอกเข้ามาใช้งานระบบได้ โดยอาจใช้การป้องกันเช่นรหัสผ่าน<br>- บันทึกเหตุการณ์ (Log file) การใช้งานของระบบไม่ต่ำกว่า 90 วัน หรือตามที่กฎหมายกำหนด<br>- ปรับปรุงอุปกรณ์เซิฟเวอร์ของโรงเรียนให้มีความปลอดภัยมากยิ่งขึ้น |

ตารางที่ 4 – 18...(ต่อ)

| ลำดับ | ภัยคุกคามทางไซเบอร์ | ความคิดเห็นของผู้ให้สัมภาษณ์ | ข้อเสนอแนะของผู้ให้สัมภาษณ์ |
|---|---|---|---|
| 2 | การฉ้อฉล | - การหลอกลวงทางสื่อสังคมออนไลน์มีมากขึ้น<br>- การโฆษณาหลอกลวงบนเว็บไซต์ | - ไม่รับเพื่อน ไม่ติดตามผู้ที่ไม่รู้จัก<br>- ไม่เปิดเผยข้อมูลสำคัญถ้าไม่จำเป็น<br>- มีสติสัมปชัญญะ อย่าหลงเชื่อโฆษณาการเล่นรับรางวัลต่าง ๆ ที่ไม่สมเหตุสมผล<br>- ไม่โลภ |
| 3 | ความพยายามรวบรวมข้อมูลของระบบ | - การทำงานด้านการทหารต้องให้ความสำคัญกับการรักษาความลับของทางราชการ โดยเฉพาะในปัจจุบันมีความพยายามรวบรวมข่าวสารผ่านทางไซเบอร์เพื่อใช้ในการโจมตีและให้ได้เปรียบในการรบ | - มีมาตรการในการเปิดเผยหรือเผยแพร่ข้อมูลทั้งข้อมูลส่วนตัวของกำลังพล และของหน่วยงานราชการ |
| 4 | การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต | - การเข้าถึงข้อมูลส่วนตัวเป็นไปได้ง่าย ดังนั้นหากมีการเข้าถึงข้อมูลได้ จะทำให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาทำการเปลี่ยนแปลง | - ไม่ควรนำข้อมูลส่วนตัวอยู่บนสื่อสังคมออนไลน์มากจนเกินความจำเป็น รวมถึงข้อมูลสำคัญต่าง ๆ ควรเก็บไว้ในพื้นที่ที่มีความปลอดภัย<br>- ไม่ล็อคอินค้างในอุปกรณ์ที่ไม่ใช่ของตน<br>- ไม่แสดงตัวตนของเรามากจนเกินไป |
| 5 | ความพยายามจะบุกรุกเข้าระบบ | - เทคโนโลยีพัฒนาไปไกลมาก ทำให้มิจฉาชีพมีความพยายามจะบุกรุกระบบ เพื่อให้ได้สิ่งที่ต้องการ | - ส่งเสริมให้ผู้ใช้สื่อสังคมออนไลน์ ใช้สื่อสังคมออนไลน์ให้ได้อย่างถูกต้องและปลอดภัย<br>- ไม่ตั้งรหัสผ่านที่สามารถคาดเดาได้โดยง่าย เช่น เบอร์โทรศัพท์ วันเกิด<br>- เปลี่ยนรหัสผ่านเป็นระยะ<br>- ไม่ควรปิด Firewall หรือ Anti-virus<br>- หลีกเลี่ยงการใช้ wifi สาธารณะ |

ตารางที่ 4 – 18...(ต่อ)

| ลำดับ | ภัยคุกคามทางไซเบอร์ | ความคิดเห็นของผู้ให้สัมภาษณ์ | ข้อเสนอแนะของผู้ให้สัมภาษณ์ |
|---|---|---|---|
| | | | - กำหนดให้อุปกรณ์มีการแจ้งเตือนทุกครั้งเมื่อมีการเข้าใช้ใหม่ในอุปกรณ์อื่น ๆ<br>- มีการสอนหรือจัดกิจกรรมสอนการป้องกันการถูกแฮกระบบขั้นพื้นฐาน |
| 6 | การบุกรุกหรือเจาะระบบได้สำเร็จ | - ขาดความเชี่ยวชาญในการป้องกัน | - ควรมีการสอนการใช้งานเกี่ยวกับการป้องกันต่างๆ เช่น เทคนิคในการตรวจสอบว่าอุปกรณ์ของเรามีการถูกแฮกหรือไม่ วิธีการตรวจสอบ URL ว่าถูกต้องไม่ผิดปกติ<br>- จัดผู้เชี่ยวชาญมาสอนถึงข้อดีข้อเสีย รายละเอียดพื้นฐานสิ่งที่ควรรู้ และสามารถพบได้ในชีวิตประจำวัน |
| 7 | โปรแกรมไม่พึงประสงค์ | - ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้าย ที่เข้ามาคัดลอกข้อมูล ควบคุมคอมพิวเตอร์ แอบล้วงข้อมูล หรือทำลายข้อมูลสำคัญต่างๆ | - การป้องกันไฟล์แปลกปลอม<br>- การไม่ใช้โปรแกรมเถื่อนเพื่อป้องกันการโจมตีจากมัลแวร์ สปายแวร์ แรนซัมแวร์ ไวรัส เวิร์ม โทรจัน ฯลฯ<br>- ไม่ควรใช้โปรแกรมที่ Crack มา<br>- การศึกษาหาความรู้เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์<br>- ตรวจสอบความผิดปกติของระบบคอมพิวเตอร์ หากมีไฟล์ผิดปกติ ต้องทำการลบทันที |
| 8 | ภัยคุกคามอื่น ๆ | โลกาภิวัตน์ทำให้เทคโนโลยีมีการพัฒนาที่ก้าวไกลมากขึ้น จึงทำให้มีภัยคุกคามอื่น ๆ ที่แฝงเข้ามาได้มากขึ้น | - มีการตรวจสอบความน่าเชื่อถือของเว็บไซต์หรือลิงค์ต่าง ๆ<br>- ติดตามข้อมูลข่าวสารสื่อสังคมออนไลน์เป็นประจำ |

ตารางที่ 4 – 18...(ต่อ)

| ลำดับ | ภัยคุกคามทางไซเบอร์ | ความคิดเห็นของผู้ให้สัมภาษณ์ | ข้อเสนอแนะของผู้ให้สัมภาษณ์ |
|---|---|---|---|
| | | | - ศึกษาหาความรู้และนำความรู้ที่มีอยู่ไปถ่ายทอดให้กับผู้อื่น<br>- อบรมเกี่ยวกับกฎหมายไซเบอร์ เพื่อจะได้มีความเข้าใจสามารถป้องกันได้ และไม่กระทำผิดกฎหมายเอง<br>- ควรใช้แอพพลิเคชั่นของประเทศเราเอง ไม่ควรใช้แอพพลิเคชั่นของประเทศอื่น |

ที่มา : ประมวลผลโดยผู้วิจัย , 2563

# บทที่ 5
# สรุปและข้อเสนอแนะ

จากการศึกษางานวิจัยเรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” มีวัตถุประสงค์เพื่อศึกษาปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ เพื่อเสนอแนะผลกระทบที่จะเกิดขึ้นจากการใช้งานไซเบอร์ โดยกลุ่มตัวอย่างที่ผู้วิจัยใช้ศึกษาความคิดเห็นเกี่ยวกับปัจจัยที่มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ คือ นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 โดยสามารถสรุปได้ดังนี้

1. การวิเคราะห์ปัจจัยที่มีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562
2. การวิเคราะห์ความเข้าใจในสถานการณ์ภัยคุกคามของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562
3. แนวทางการพัฒนาหลักสูตรการรักษาความปลอดภัยทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า
4. ข้อเสนอแนะ
5. ข้อจำกัดในการวิจัย

## การวิเคราะห์ปัจจัยที่มีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562

การศึกษาปัจจัยที่มีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 นั้นได้ทำการศึกษาปัจจัยดังต่อไปนี้

1. ปัจจัยการศึกษาของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าในแต่ละชั้นปี
2. ปัจจัยการศึกษาของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าในแต่ละหลักสูตร
3. ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

การศึกษาปัจจัยที่มีผลต่อความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 นี้เป็นการวิจัยเชิงปริมาณ (Quantitative Research) ด้วยการวิจัยเชิงสำรวจ (Survey Research) ประชากร คือ นักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ประจำปีการศึกษา 2562 ขนาดตัวอย่าง 300 นาย เครื่องมือที่ใช้ในการวิจัย คือ

แบบสอบถามใช้วิธีกลุ่มตัวอย่างกรอกแบบสอบถามด้วยตนเอง (Self-Administered Questionnaire) โดยใช้สถิติเชิงพรรณนา และสถิติเชิงอนุมานในการวิเคราะห์ข้อมูล

1. สรุปผลข้อมูลลักษณะทางประชากร

กลุ่มตัวอย่างเป็นนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า 5 ชั้นปี โดยนักเรียนชั้นปีที่ 1 มีจำนวนมากที่สุดคือ 63 นาย คิดเป็นร้อยละ 21 รองลงมา ร้อยละ 20.3 คือ นักเรียนนายร้อยชั้นปีที่ 3 และชั้นปีที่ 5 มีจำนวน 61 นาย นักเรียนนายร้อยชั้นปีที่ 4 จำนวน 60 นาย คิดเป็นร้อยละ 20 และน้อยที่สุดคือนักเรียนนายร้อยชั้นปีที่ 2 จำนวน 55 นาย คิดเป็นร้อยละ 18.3

กลุ่มตัวอย่างส่วนใหญ่เรียนหลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมเพื่อการพัฒนา จำนวน 77 นาย คิดเป็นร้อยละ 25.7 รองลงมา คือหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี จำนวน 60 นาย คิดเป็นร้อยละ 20 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมแผนที่ จำนวน 33 นาย คิดเป็นร้อยละ 11 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมโยธา และหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์ จำนวน 31 นาย เท่ากัน คิดเป็นร้อยละ 10.3 หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร กับหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมอุตสาหการ มีจำนวนเท่ากันคือ 24 นาย คิดเป็นร้อยละ 8 และน้อยที่สุดคือหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล จำนวน 20 นาย คิดเป็นร้อยละ 6.7 ตามลำดับ

2. สรุปผลข้อมูลประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์

กลุ่มตัวอย่างมีประสบการณ์เกี่ยวกับภัยคุกคามไซเบอร์ในประเด็น “นักเรียนเคยได้รับโฆษณาที่ไม่พึงประสงค์จะได้รับ” สูงที่สุด (ร้อยละ 79) รองลงมาคือ “เคยได้รับผลกระทบจากไวรัสที่ทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย” (ร้อยละ 75.3) “ติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวเข้ามา”(ร้อยละ 66) “การก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ” (ร้อยละ 63.7) “ได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง” (ร้อยละ 61.7) “หลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ” (ร้อยละ 50) “ถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์” (ร้อยละ 40.3) “ผู้อื่นเข้ามาใช้งานคอมพิวเตอร์ของนักเรียนได้โดยไม่รู้ตัว” (ร้อยละ 39) “ขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน” (ร้อยละ 26) “ไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นจะได้รับข้อความ “เรียกค่าไถ่”(ร้อยละ 21.7) ตามลำดับ

หากจัดประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์เป็น 3 ระดับ พบว่า กลุ่มตัวอย่างส่วนมาก มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ในระดับปานกลาง ร้อยละ 64.3 รองลงมาคือ ร้อยละ 21.7 มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับน้อย และร้อยละ 14 มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ระดับมาก ตามลำดับ

3. สรุปผลข้อมูลความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์

ในภาพรวมกลุ่มตัวอย่างมีความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์ ในระดับปานกลาง (3.361) โดยด้านที่มีกลุ่มตัวอย่างมีความตระหนักในระดับมากคือ ด้านการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม (3.607) ส่วนกลุ่มตัวอย่างที่มีความตระหนักในระดับปานกลางคือ ด้านโปรแกรมประสงค์ร้าย (3.337) และด้านการโจรกรรมข้อมูล (3.140) เมื่อพิจารณารายละเอียดแต่ละด้านพบว่า

ด้านการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม ประเด็นที่มีความตระหนักในระดับมากคือ การไม่เผยแพร่ข่าวลือในทางลบของผู้อื่นทางสื่อสังคมออนไลน์ และการไม่เผยแพร่ข้อมูลส่วนบุคคลของผู้อื่นทางสื่อสังคมออนไลน์ (3.78) การไม่ทำให้ผู้อื่นอับอายหรือเสียชื่อเสียงทางสื่อสังคมออนไลน์ และการไม่ล้อเลียนรูปร่างหน้าตาของผู้อื่นทางสื่อสังคมออนไลน์ (3.74) การไม่แชร์ข้อมูลที่ไม่ถูกต้องทางสื่อสังคมออนไลน์ (3.71) การไม่กีดดันผู้อื่นทางสื่อสังคมออนไลน์ (3.70) การไม่ใช้ข้อความหยาบคายด่าว่าผู้อื่นทางสื่อสังคมออนไลน์ (3.54)

ด้านโปรแกรมประสงค์ร้าย ประเด็นที่มีความตระหนักในระดับมากคือ การป้องกันตนเองด้วยโปรแกรมป้องกันไวรัส (3.53) และการป้องกันตนเองจากโปรแกรมโฆษณา (3.53)

ด้านการจารกรรมข้อมูล ประเด็นที่มีความตระหนักในระดับมากคือ การตั้งรหัสผ่านที่ดีเพื่อป้องกันการจารกรรมข้อมูล (3.65) การป้องกันโจรกรรมข้อมูลจากการเข้าถึงอุปกรณ์ฮาร์ดแวร์ (3.60)

4. สรุปผลข้อมูลการทดสอบสมมติฐาน ผลการทดสอบสมมติฐาน พบว่า

ปัจจัยด้านชั้นปีการศึกษา มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า โดยนักเรียนนายร้อยชั้นปีที่ 1 มีความตระหนักถึงภัยคุกคามทางไซเบอร์มากกว่านักเรียนชั้นปีอื่น ๆ อย่างมีนัยสำคัญ การระบุกลุ่มตัวอย่างได้ดังนี้สามารถนำไปวิเคราะห์เพื่อหาแนวทางกำหนดกลุ่มเป้าหมาย และวิธีป้องกัน เพื่อลดความเสี่ยงจากภัยคุกคามของการโจมตีทางไซเบอร์ สร้างความตระหนักและความเข้าใจเพื่อลดผลกระทบที่อาจเกิดขึ้นจากการใช้งานและใช้ชีวิตประจำวัน

ปัจจัยด้านหลักสูตรการศึกษา พบว่าไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ดังนี้ข้อมูลดังกล่าวสามารถนำไปสร้างแนวทางในการจัดการศึกษาอบรมเกี่ยวกับการสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์เพิ่มในแต่ละหลักสูตรได้ไม่ต่างกัน

ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า โดยจะเห็นได้ว่าผู้ที่มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์น้อย จะมีความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์มากอย่างมีนัยสำคัญ อาจแสดงให้เห็นว่ากลุ่มตัวอย่างที่มีความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ จะคอยระวังป้องกันตนเองจากภัยต่าง ๆ ที่เกิดขึ้น ส่งผลให้มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์น้อย

## การวิเคราะห์ความเข้าใจในสถานการณ์ภัยคุกคามของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562

จากการสัมภาษณ์นักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 ในเรื่องภัยคุกคามทางไซเบอร์นั้น สามารถวิเคราะห์ได้ดังนี้

1. เนื้อหาที่เป็นภัยคุกคาม (Abusive Content) พบว่านักเรียนนายร้อยมีความเข้าใจเนื้อหาที่เป็นภัยคุกคามทั้งการเป็นผู้เขียนเนื้อหาที่ไม่เหมาะสมลงบนสื่อสังคมออนไลน์ หรือเข้าไปอ่านในสื่อที่ไม่เหมาะสม โดยมีข้อเสนอแนะให้ระมัดระวังในการใช้สื่อ และควรมีการวิเคราะห์ข้อมูลของตนเองให้ดีก่อนทำการเผยแพร่ นอกจากนี้ยังมีความเห็นว่า โรงเรียนนายร้อยพระจุลจอมควรมีการบล๊อคเว็บไซต์ที่ไม่เหมาะสมอีกด้วย

2. การโจมตีสภาพความพร้อมใช้งานของระบบ (Availability) พบว่านักเรียนนายร้อยมีความรู้ความเข้าใจภัยคุกคาม ที่เกิดจากการโจมตีสภาพความพร้อมใช้ของระบบ ซึ่งจะทำให้การบริการต่าง ๆ ของระบบไม่สามารถทำงานได้ โดยเห็นว่าควรมีการกำหนดมาตรการใช้อินเทอร์เน็ตในองค์กร มีอุปกรณ์ป้องกันระบบเครือข่ายที่ทำหน้าที่เป็นตัวกรองข้อมูล และผู้ดูแลระบบควรมีการตรวจสอบการเข้าใช้งานข้อมูล (Log file) อย่างสม่ำเสมอ

3. การฉ้อฉล (Fraud) คือการฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ พบว่านักเรียนมีความรู้ความเข้าใจว่าการหลอกลวงทางสื่อสังคมออนไลน์มีมากขึ้น รวมถึงมีการโฆษณาหลอกลวงบนเว็บไซต์ ดังนั้นจึงมีแนวทางการป้องกันโดยการไม่รับเพื่อนหรือไม่รับผู้ติดตามที่ไม่รู้จัก ไม่เปิดเผยข้อมูลที่มีความสำคัญ มีสติสัมปชัญญะ ไม่หลงเชื่อไปกับสิ่งที่ไม่สมเหตุสมผล และข้อหนึ่งที่น่าสนใจคือการไม่โลภซึ่งจะเป็นการแก้ปัญหาการถูกฉ้อฉลได้อย่างมีประสิทธิภาพ เนื่องจากการล่อลวงต่าง ๆ นั้นมักใช้ความโลภของเหยื่อเป็นข้อเสนอให้หลงเชื่อและยอมรับไปกับสิ่งที่ไม่สมเหตุสมผลนั้น ๆ

4. ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering) โดยผู้ไม่ประสงค์ดีพยายามรวบรวมจุดอ่อนของระบบ เพื่อใช้ในการล่อลวง หรือโจมตี โดยจากการสัมภาษณ์นักเรียนนายร้อยมีความตระหนักถึงความสำคัญของการรักษาความลับของทางราชการ โดยเสนอให้มีมาตรการในการไม่เปิดเผยหรือเผยแพร่ข้อมูลทั้งส่วนตัวและของหน่วยงาน

5. การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) จากการสัมภาษณ์พบว่านักเรียนนายร้อย มีความตระหนักถึงภัยคุกคามในการเข้าถึงข้อมูลส่วนตัวซึ่งในปัจจุบันสามารถทำได้ง่ายผ่านทางอินเทอร์เน็ต ดังนั้นจึงเสนอว่าไม่ควรนำข้อมูลส่วนตัวมาอยู่ในสื่อสังคมออนไลน์เกินความจำเป็นและอาจป้องกันด้วยการออกจากระบบ (Log out) ทุกครั้งที่ใช้งาน

6. ความพยายามบุกรุกเข้าระบบ (Intrusion Attempts) จากการสัมภาษณ์นักเรียนนายร้อยมีความตระหนักถึงภัยคุกคามทางไซเบอร์ ที่มาพร้อมกับเทคโนโลยีที่พัฒนาไปอย่างรวดเร็ว ส่งผลให้เกิดมีช่องทางใหม่สำหรับมิจฉาชีพพยายามที่จะบุกรุกระบบ เพื่อให้ได้สิ่งที่ต้องการ ดังนั้นแนวทางการป้องกันคือ ส่งเสริมให้ผู้ใช้สื่อสังคมออนไลน์มีความรู้ในการใช้อย่างถูกต้อง เช่น

มีการตั้งรหัสผ่านที่คาดเดาได้ยาก เปลี่ยนรหัสผ่านให้บ่อยครั้ง ไม่ปิด Firewall หรือ Anti-Virus รวมถึงไม่ใช้เครือข่าย Wi-fi สาธารณะกับข้อมูลที่มีความสำคัญ นอกจากนี้ยังเห็นว่าควรมีการอบรมพื้นฐานการรักษาความปลอดภัยของไซเบอร์ เพื่อใช้ในชีวิตประจำวัน และสามารถนำไปถ่ายทอดให้ผู้อื่นได้

7. การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) เป็นภัยคุกคามที่เกิดกับระบบที่ถูกบุกรุก/เจาะระบบสำเร็จแล้ว และระบบถูกครอบครองโดยผู้ไม่ได้รับอนุญาต จากการสัมภาษณ์นักเรียนนายร้อยมีความเข้าใจว่าการขาดความเชี่ยวชาญในการป้องกัน เป็นจุดอ่อนของการที่ระบบจะถูกเจาะระบบได้สำเร็จ แต่อย่างไรก็ตาม การบุกรุกหรือเจาะระบบได้สำเร็จแล้ว ผู้บุกรุกอาจไม่แสดงอันตรายใด ๆ กับระบบ แต่อาจแฝงตัวเพื่อรวบรวมข้อมูลที่สำคัญหรือทำลายระบบเมื่อต้องการได้ ดังนั้นแนวทางการป้องกันที่นักเรียนเสนอคือ ควรให้มีการสอนการใช้การป้องกันต่าง ๆ รวมถึงมีเทคนิคและอุปกรณ์ตรวจสอบว่าระบบถูกแฮคหรือไม่ เป็นต้น นอกจากนี้ยังเสนอให้มีการจัดผู้เชี่ยวชาญมาสอน ทั้งรายละเอียดพื้นฐาน และสิ่งที่ควรทราบในการดำเนินงานในชีวิตประจำวัน

8. โปรแกรมไม่พึงประสงค์ (Malicious Code) จากการสัมภาษณ์พบว่า ผู้ถูกสัมภาษณ์มีความตระหนักรู้ภัยคุกคามของโปรแกรมไม่พึงประสงค์เป็นอย่างดี รวมทั้งมีประสบการณ์จากการทำร้ายระบบของโปรแกรมไม่พึงประสงค์ ประเภทไวรัสด้วย ดังนั้นจึงมีข้อเสนอแนะให้ป้องกันไฟล์แปลกปลอม ไม่ใช้โปรแกรมผิดลิขสิทธิ์ ไม่นำโปรแกรมที่ถอดรหัสมาใช้ รวมถึงการสังเกตความผิดปกติของการทำงานของคอมพิวเตอร์

9. ภัยคุกคามอื่น ๆ เป็นภัยคุกคามนอกเหนือจากที่กล่าวข้างต้น ซึ่งรวมถึงภัยคุกคามทำร้ายกันด้วยข้อมูลข่าวสาร ซึ่งพบว่าผู้ให้สัมภาษณ์เข้าใจถึงโลกในยุคโลกาภิวัฒน์ที่ส่งผลให้เทคโนโลยีมีการพัฒนาที่ก้าวไกลมากขึ้น อาจมีภัยคุกคามอื่นแฝงเข้ามา นอกจากนี้ยังรวมถึงภัยคุกคามทางสื่อสังคมออนไลน์ เช่น การดูถูก เหยียดหยาม ให้ร้ายผู้อื่น การป้องกันภัยคุกคามประเภทนี้ผู้ให้สัมภาษณ์เสนอให้มีการตรวจสอบความน่าเชื่อเถือของเว็บไซต์, ติดตามข้อมูลข่าวสารอยู่เสมอ, ศึกษาหาความรู้และนำไปถ่ายทอดให้ผู้อื่น รวมถึงอบรมเกี่ยวกับกฎหมายการกระทำผิดทางไซเบอร์เพื่อให้มีความรู้ความเข้าใจไม่กระทำผิดกฎหมายเอง และเรื่องที่น่าสนใจคือ ประเทศควรมีการพัฒนาแอพพลิเคชั่นขึ้นมาใช้เอง เพราะการใช้แอพพลิเคชั่นต่างชาติ อาจทำให้มีการรั่วไหลของข้อมูลที่มีความสำคัญ หรือหากเกิดความขัดแย้งเกิดขึ้นประเทศไม่ได้รับอนุญาตให้ใช้แอพพลิเคชั่นก็จะทำให้เกิดความชะงักงันของระบบสารสนเทศของประเทศเป็นส่วนรวมได้ หากไม่มีแนวทางอื่นรองรับ

## ข้อเสนอแนวทางการพัฒนาหลักสูตรวิทยาศาสตรบัณฑิต สาขาความมั่นคงปลอดภัยทางไซเบอร์

แม้ว่าโรงเรียนนายร้อยพระจุลจอมเกล้า จะได้เริ่มดำเนินการจัดทำหลักสูตรวิทยาศาสตรบัณฑิต สาขาความมั่นคงปลอดภัยทางไซเบอร์ เป็นเวลา 1 ปี โดยผู้เข้ารับการศึกษาคือนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 2 แต่อย่างไรก็ตามเทคโนโลยีสารสนเทศมีการพัฒนาอย่างรวดเร็วแบบก้าวกระโดด การพัฒนาหลักสูตรดังกล่าวจึงไม่สามารถหยุดนิ่งต้องมีการ

พัฒนาปรับปรุงอยู่เสมออย่างต่อเนื่อง และรวดเร็วทันต่อสถานการณ์ในปัจจุบัน รวมทั้งมีการเตรียมความพร้อมสำหรับอนาคต เพื่อให้นักเรียนนายร้อยพระจุลจอมเกล้า มีความรู้ ทักษะ ที่จำเป็นในการสร้างความเข้าใจและความเชี่ยวชาญในความมั่นคงปลอดภัยทางไซเบอร์ สามารถระบุความเสี่ยง ลดความเสี่ยงที่อาจเกิดขึ้นได้ รวมถึงต้องมีความรู้ความเข้าใจด้านโครงสร้างพื้นฐานของเทคโนโลยีสารสนเทศ การประยุกต์ใช้ข้อมูลสารสนเทศและการควบคุมด้านความปลอดภัยให้ได้อย่างมีผลสัมฤทธิ์ทั้งในด้านการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ของข้อมูลสารสนเทศ (Availability) สามารถจัดการเทคโนโลยีสารสนเทศได้อย่างเหมาะสมสอดคล้องกับนโยบายของกองทัพบก ตามระเบียบข้อบังคับของกฎหมาย รวมถึงการเรียนรู้การตรวจหาการโจมตีเพื่อจัดทำเป็นรายงานเชิงอาชญากรรมได้ เพื่อป้องกันการโจมตีในอนาคต โดยทักษะที่ได้จะต้องจัดให้อยู่ในระดับสากล ส่งเสริมและพัฒนาให้เกิดผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางไซเบอร์ ดังนั้นหลักสูตรดังกล่าวจึงควรมีการประเมินและทำการทบทวนหลักสูตรให้เกิดความเหมาะสมและทันสมัยอยู่เสมอ โดยกำหนดแนวทางที่ชัดเจน จากการศึกษาเรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” นี้ ทำให้ผู้วิจัยได้ทราบข้อมูลเบื้องต้นเกี่ยวกับความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า เพื่อเสนอเป็นแนวทางการพัฒนาหลักสูตรวิทยาศาสตรบัณฑิต สาขาความมั่นคงปลอดภัยทางไซเบอร์ เพิ่มเติมดังนี้

**1. สอดคล้องกับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสากล**

จากการกำเนิดของโลกาภิวัตน์ทำให้หลาย ๆ ระบบเกิดการเชื่อมโยงเข้าไว้ด้วยกัน ดังที่เห็นในปัจจุบัน เทคโนโลยีสารสนเทศทำให้โลกเชื่อมกันดังกล่าวภัยคุกคามทางด้านไซเบอร์ก็สามารถเชื่อมโยงไปถึงกันหมดเช่นเดียวกัน การพัฒนาหลักสูตรวิทยาศาสตรบัณฑิต สาขาความมั่นคงปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า จึงต้องสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสากล ซึ่งในปัจจุบันมีการจัดทำมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์เกิดขึ้นหลายองค์กร การพัฒนาหลักสูตรจึงควรมีการศึกษามาตรฐานต่าง ๆ และเลือกมาตรฐานที่เหมาะสมเพื่อใช้เป็นแนวทางในการกำหนดวิชาต่าง ๆ ในหลักสูตรเพื่อให้สอดคล้องกับมาตรฐานเหล่านั้น และมีการจัดทำคลังข้อสอบเพื่อเตรียมการให้นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าได้ศึกษา เพื่อเตรียมการสอบตามมาตรฐานของสากล รวมถึงการจัดหางบประมาณในการสอบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสากล และในอนาคตโรงเรียนนายร้อยพระจุลจอมเกล้าอาจสามารถพัฒนาเป็นสถาบันอีกแห่งหนึ่งที่ใช้ในการทดสอบมาตรฐานความปลอดภัยทางไซเบอร์ในระดับประเทศ, ระดับอาเซียน หรือแม้แต่ระดับโลกได้

**2. ความรู้พื้นฐานทางเทคโนโลยีสารสนเทศที่จำเป็น**

การปรับปรุงหลักสูตรวิทยาศาสตรบัณฑิต สาขาความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบัน โรงเรียนนายร้อยพระจุลจอมเกล้า ได้ทำการปรับหลักสูตรมาจากหลักสูตรวิทยาศาสตร์บัณฑิตสาขาวิทยาการคอมพิวเตอร์ ซึ่งเดิมเป็นหลักสูตรหลักของนักเรียนนายร้อยพระจุลจอมเกล้า ซึ่งจะจบการศึกษาไปจะเป็นกำลังหลักในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของกองทัพบก เมื่อมีการปรับปรุงหลักสูตรโดยการยกเลิกบางวิชา และนำวิชาการเกี่ยวกับความมั่นคงปลอดภัย

ทางไซเบอร์เข้ามาเสริม ผู้วิจัยมีความเห็นว่าจะทำให้นักเรียนนายร้อยพระจุลจอมเกล้าที่จบหลักสูตรไม่ได้รับความรู้พื้นฐานทางเทคโนโลยีสารสนเทศ ที่ต้องใช้ในการทำงานในอนาคตที่เกี่ยวกับวิทยาการคอมพิวเตอร์เพียงพอ เพราะอย่างไรก็ตาม กองทัพบกก็ยังมีความจำเป็นต้องใช้กำลังพลที่จบการศึกษาในหลักสูตรเหล่านี้ไปปฏิบัติหน้าที่ที่เกี่ยวข้องกับสายงานสารสนเทศของกองทัพบก และในปัจจุบันเทคโนโลยีสารสนเทศก็เข้าไปมีบทบาทในเกือบทุกสายงาน สำหรับวิชาที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ ที่เสริมเข้ามาก็ไม่เพียงพอที่จะปฏิบัติงานที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างเต็มรูปแบบ เพื่อให้สอดคล้องกับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสากลได้ อีกทั้งนายทหารที่จบหลักสูตรก็ยังมีความจำเป็นต้องทำงานสารสนเทศอื่น ๆ ตามที่หน่วยกำหนด จึงควรแยกหลักสูตรการศึกษาให้ชัดเจน ซึ่งอาจแยกเป็นคนละหลักสูตรหรือหลักสูตรเดียวกันแต่แยกแขนงหลักสูตร โดยมีแขนงวิทยาการคอมพิวเตอร์ ที่เน้นเกี่ยวกับการทำงานด้านสารสนเทศให้กับกองทัพบก เช่น การวิเคราะห์และออกแบบระบบงานสารสนเทศ การพัฒนาโปรแกรมเพื่อใช้งานสารสนเทศต่าง ๆ ของกองทัพบก ฯลฯ และแขนงความมั่นคงปลอดภัยทางไซเบอร์เป็นการเฉพาะเพื่อเน้นด้านการดูแลระบบเครือข่าย การป้องกันและแก้ปัญหาภัยคุกคามทางไซเบอร์ในระดับต่าง ๆ ให้กับกองทัพบก เป็นต้น ซึ่งจะช่วยให้กองทัพบกไม่ขาดแคลนบุคลากรในการดำเนินการในทุกด้านที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ และการรักษาความมั่นคงปลอดภัยทางไซเบอร์

**3. สื่อการเรียนการสอนที่เหมาะสม**

เป็นที่ทราบกันดีอยู่แล้วว่าการศึกษาอบรมจำเป็นเป็นต้องมีอุปกรณ์เครื่องมือ ซึ่งเป็นส่วนสำคัญที่จะต้องมีการจัดหา เพื่อเป็นองค์ประกอบในการจัดทำสื่อการเรียนการสอนที่เหมาะสม ซึ่งหลักสูตรการรักษาความปลอดภัยทางไซเบอร์ นอกจากอุปกรณ์การสอนโดยทั่วไปแล้วยังต้องใช้เครื่องมืออื่น ๆ ที่เกี่ยวข้องกับการรับมือกับภัยคุกคามทางไซเบอร์ ทั้งการจำลองเหตุการณ์สถานการณ์ต่าง ๆ เพื่อให้ผู้เรียนได้ฝึกปฏิบัติระบบเครือข่ายที่เป็นเครือข่ายจำลองในระบบปิดเพื่อป้องกันภัยคุกคามที่ทดลองใช้ในแต่ละสถานการณ์เผยแพร่ไปสู่ระบบอื่น ผู้เรียนจะต้องรู้จักเครื่องมือต่าง ๆ ทั้งฮาร์ดแวร์ เช่น เซิร์ฟเวอร์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เทคโนโลยีสารสนเทศประเภทต่าง ๆ ซอฟแวร์ ทั้งซอฟแวร์ระบบและแอพพลิเคชั่นที่ใช้งานทั่วไป อีกทั้งซอฟแวร์เพื่อใช้ในการศึกษาหาช่องโหว่ ซอฟแวร์ประสงค์ร้าย ซอฟแวร์แอนตี้ไวรัส ซอฟแวร์ในการคำนวณรหัสผ่าน เป็นต้น นอกจากนี้ยังรวมถึงอุปกรณ์เครือข่ายต่าง ๆ และอุปกรณ์ที่ผู้รุกรานใช้ เพื่อให้ผู้เรียนตระหนักรู้การใช้ภัยคุกคามแบบต่าง ๆ เช่น อุปกรณ์ดักฟัง การทำงานของคีย์ลอกเกอร์ เป็นต้น

**4. การพัฒนาอาจารย์ผู้สอน**

หัวใจของการศึกษาอบรม นอกจากผู้เรียนแล้วก็คือผู้สอนที่ต้องถ่ายทอดความรู้ให้ผู้เรียนเกิดความรู้ความเข้าใจในศาสตร์นั้น ๆ และเนื่องจากหลักสูตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นเรื่องใหม่ของโรงเรียนนายร้อยพระจุลจอมเกล้าที่จะเปิดหลักสูตรฯ การพัฒนาศักยภาพของอาจารย์จึงเป็นสิ่งที่จำเป็นอย่างยิ่ง การเพิ่มพูนความรู้ความสามารถและทักษะในการปฏิบัติงานของอาจารย์ให้ได้ผลดีให้มีประสิทธิผลและประสิทธิภาพจะช่วยบรรลุเป้าหมายของการพัฒนาหลักสูตรด้วยเช่นกัน จึงควรมีดำเนินการพัฒนาอาจารย์ผู้สอนในรูปแบบต่าง เช่น

4.1 การผลิตอาจารย์ให้มากขึ้นเนื่องจากหลักสูตรการรักษาความปลอดภัยทางไซเบอร์เป็นเรื่องใหม่ อาจต้องใช้อาจารย์ที่ศึกษาในด้านนี้มาโดยเฉพาะ

4.2 การจัดสรรทุนเพื่อศึกษาต่อทั้งในและนอกประเทศ รวมถึงการศึกษาแบบออนไลน์

4.3 การบริหารจัดการให้อาจารย์มีความรู้ความสามารถ มีการพัฒนาตนเองอยู่เสมอ และยังทำหน้าที่รับราชการในโรงเรียนนายร้อยพระจุลจอมเกล้าต่อไป และการจัดการให้มีบุคลากรรุ่นใหม่ทดแทนเพื่อการสอนอย่างต่อเนื่อง

4.4 ความร่วมมือกับสถาบันในระดับอุดมศึกษาอื่น ๆ ทั้งในและต่างประเทศเพื่อให้เกิดเครือข่ายความร่วมมือด้านทรัพยากรบุคคล มีการเชิญผู้เชี่ยวชาญแลกเปลี่ยนอาจารย์ และมีการจัดประชุมวิชาการ เพื่อเป็นการสนับสนุนและยกระดับด้านคุณภาพของการผลิตบุคลากรด้านการสอนให้มีประสิทธิภาพต่อไป

**5. ทักษะที่ควรได้รับจากหลักสูตรวิทยาศาสตรบัณฑิต สาขาการรักษาความมั่นคงปลอดภัยทางไซเบอร์**

นักเรียนนายร้อยพระจุลจอมเกล้าควรมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ดังนี้

5.1 ด้านภัยคุกคาม การโจมตี และช่องโหว่

5.1.1 มีความรู้ความเข้าใจเกี่ยวกับชนิดและประเภทต่าง ๆ ของซอฟแวร์ประสงค์ร้าย (Malware) เช่น ไวรัส (Virus) ซอฟแวร์เรียกค่าไถ่ (Ransomware) หนอนคอมพิวเตอร์ (Worm) โทรจัน (Trojan) เป็นต้น

5.1.2 เปรียบเทียบและระบุความแตกต่างของการโจมตีประเภทต่าง ๆ เช่น Social engineering, การโจมตีซอฟแวร์และการบริการอื่น ๆ (Application/service attacks), การโจมตีเครือข่ายไร้สาย (Wireless attacks), การโจมตีการเข้ารหัส (Cryptographic attacks)

5.1.3 มีความรู้ความเข้าใจประเภทของการบุกรุก เช่น Script Kiddies, Hacktivist, Insiders, Competitions

5.1.4 มีความรู้เกี่ยวกับช่องโหว่ของระบบได้ และสามารถเข้าใจผลกระทบที่เกิดจากช่องโหว่นั้นได้

5.1.5 สามารถอธิบายภาพรวมการเจาะระบบให้ผู้บังคับบัญชารับทราบได้

5.2 ด้านเทคโนโลยีสารสนเทศ

5.2.1 มีความรู้เกี่ยวกับอุปกรณ์ระบบเครือข่ายที่มีความมั่นคงปลอดภัย เช่น Firewall, VPN concentrator, Router เป็นต้น

5.2.2 มีความรู้เกี่ยวกับซอฟแวร์สำหรับประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างเหมาะสม

5.2.3 มีความรู้เกี่ยวกับแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศขั้นพื้นฐาน

5.3 ด้านสถาปัตยกรรมและการออกแบบ

5.3.1 มีความรู้เกี่ยวกับแนวคิดสถาปัตยกรรมเครือข่ายที่ปลอดภัย และการออกแบบระบบที่ปลอดภัยได้

5.3.2 สามารถแนะนำการพัฒนาแอปพลิเคชั่นที่ปลอดภัยได้

5.3.3 สามารถดำเนินการเพื่อลดความเสี่ยงด้วยระบบอัตโนมัติได้

5.3.4 ให้ความสำคัญของการรักษาความปลอดภัยทางกายภาพ

5.4 ด้านการจัดการข้อมูลประจำตัวและการเข้าถึง

5.4.1 มีความรู้เกี่ยวกับความแตกต่างของการพิสูจน์ตัวตนและการจัดการการเข้าถึงระบบ (Access management)

5.4.2 มีความรู้เกี่ยวกับระบบพิสูจน์ตัวตนและการเข้าถึงระบบ

5.4.3 การบริหารจัดการบัญชีผู้ใช้ (Account Management)

5.5 ด้านการจัดการความเสี่ยง

5.5.1 กำหนดความสำคัญของนโยบาย แผนการดำเนินงาน ขั้นตอนการปฏิบัติที่ส่งผลกระทบกับความปลอดภัยของหน่วย

5.5.2 วิเคราะห์ปัจจัยที่มีผลกระทบกับหน่วย

5.5.3 จัดทำกระบวนการการจัดการความเสี่ยง

5.5.4 มีความรู้เกี่ยวกับการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น

5.5.5 การเก็บรวบรวมหลักฐานทางดิจิทัลพื้นฐาน

5.5.6 จัดทำแผนกู้คืนภัยพิบัติ

5.5.7 จัดทำนโยบายความเป็นส่วนตัวและการส่งข้อมูลออกไปภายนอก

5.6 การเข้ารหัส

5.6.1 มีความรู้การเข้ารหัสขั้นพื้นฐาน

5.6.2 มีคามรู้เกี่ยวกับความปลอดภัยของระบบเครือข่ายไร้สาย

5.7 ด้านการตอบโต้เหตุการณ์บนโลกไซเบอร์

5.7.1 มีความรู้เกี่ยวกับข้อมูลภัยคุกคามเพื่อกำหนดผลกระทบของเหตุการณ์และรู้จักชุดเครื่องมือที่เหมาะสม สร้างกลยุทธ์การสื่อสาร พร้อมแนวทางปฏิบัติในการตอบโต้ได้

5.7.2 สามารถดำเนินการและสรุปแนวทางปฏิบัติที่ดีที่สุด ป้องกันผลกระทบต่อหน่วยได้

5.8. ด้านกฎหมาย/ศีลธรรม

ปัจจุบันมีกฎหมายที่เกี่ยวข้องกับสื่อสังคมออนไลน์ เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ ซึ่งนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้าควรได้รู้จักเข้าใจ และป้องกันไม่กระทำการใด ๆ ที่นำมาซึ่งการผิดพระราชบัญญัติที่เกี่ยวข้องกับการกระทำผิดดังกล่าว จึงควรมีหลักสูตรทางด้านกฎหมายแทรกเข้าไปในหลักสูตรด้วย รวมถึงในอนาคตหากนักเรียนมีความรู้ความสามารถในเรื่องที่เกี่ยวกับไซเบอร์มากขึ้น ก็ไม่ควรกระทำการใด ๆ ที่อาจส่งผลเสียต่อผู้อื่น ดังนั้นในหลักสูตรจึงควรมีการอบรมในเรื่องของศีลธรรม จรรยา ความรู้สึกผิดชอบชั่วดี เพื่อให้นักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า จบการศึกษาโดยมีวิชาความรู้เกียรติ วินัย ศักดิ์ศรี เป็นความภาคภูมิใจของสถาบันต่อไป

## ข้อเสนอแนะ

การทำวิจัยครั้งต่อไป ในการทำการวิจัยเกี่ยวกับภัยคุกคามทางไซเบอร์ มีข้อเสนอแนะดังนี้

1. ควรศึกษาปัจจัยด้านความรู้ทางด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเป็นปัจจัยที่ส่งผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของกลุ่มตัวอย่าง

2. ควรศึกษาการใช้งานของกลุ่มตัวอย่างว่ามีการใช้งานทางไซเบอร์มากน้อยเพียงใด ประเด็นใดบ้าง เพื่อศึกษาความเสี่ยงของภัยคุกคามทางไซเบอร์

3. ควรจะใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยการสัมภาษณ์กลุ่ม (Focus Group Interview) หรือการสัมภาษณ์เจาะลึก (In-depth Interview) เพื่อศึกษาความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ที่เกี่ยวข้องกับกลุ่มตัวอย่าง เช่น ผู้บังคับบัญชา อาจารย์ เพื่อให้ได้ข้อมูลที่รอบด้านครบทุกมิติมากยิ่งขึ้น

4. ควรมีการศึกษานโยบายของรัฐ กระทรวงกลาโหม กองทัพบก และองค์กรต่าง ๆ ที่เกี่ยวกับการป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต

## ข้อจำกัดในการวิจัย

การศึกษาในครั้งนี้มีข้อจำกัดด้านระยะเวลาในการค้นคว้า ซึ่งอาจทำให้การศึกษาปัจจัยที่มีผลกระทบต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ในข้อมูลเชิงลึกได้ไม่เพียงพอ

# บรรณานุกรม

## ภาษาไทย

### หนังสือ

จตุชัย แพงจันทร์. Master in Security.นนทบุรี : บริษัทไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์ จำกัด, 2550.

### วิทยานิพนธ์ รายงานการวิจัย เอกสารวิจัย

กุลวดี ราชภักดี. “ความตระหนักและการปฏิบัติเกี่ยวกับการประหยัดพลังงานไฟฟ้าของนักศึกษาในหอพักสถาบันอุดมศึกษา เขตกรุงเทพมหานคร”. สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง, 2545.

อนุสรณ์ กาลดิษฐ์. “การศึกษาความรู้ และความตระหนักของนักศึกษาที่มีต่อปัญหาสิ่งแวดล้อมในห้องปฏิบัติการ วิศวอุตสาหการ คณะวิศวกรรมศาสตร์ในเขตกรุงเทพมหานคร”. ปริญญานิพนธ์, มหาวิทยาลัยศรีนครินทรวิโรฒ, 2548.

สุกัญญา ช้างแก้ว. “การเสริมสร้างความมั่นคงด้านเทคโนโลยีของกองทัพบก” . เอกสารวิจัยส่วนบุคคล, วิทยาลัยการทัพบก, 2555.

สุธาเทพ รุณเรศ. “ปัจจัยที่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของผู้ใช้อินเทอร์เน็ตในกรุงเทพมหานคร” . มหาวิทยาลัยธรรมศาสตร์ วิทยาลัยนวัตกรรม, 2561.

### เอกสารไม่ตีพิมพ์

สภาความมั่นคงแห่งชาติ,สำนักนายกรัฐมนตรี.“นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ.2562 – 2564)”. 2562.

### ฐานข้อมูลอิเล็กทรอนิกส์

ซอฟแวร์พาร์ค . “โครงการพัฒนาผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ ด้วยมาตรฐานในระดับสากล (IT Cyber Security Certification Program)” . (ออนไลน์) . เข้าถึงได้จาก : http://www.cybersecurity-cert.com/img/doc/detail.pdf

ปริญญา หอมเอนก. “มาตรฐานสากลทางด้านความปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ CIO ควรรู้เพื่อนำมาใช้เป็นแนวทางปฏิบัติในองค์และกลยุทธ์ CIO กับการบริหารระบบความปลอดภัยเทคโนโลยีสารสนเทศในองค์กรสมัยใหม่”. (ออนไลน์) . เข้าถึงได้จาก : https://www.acisonline.net/?p=1849

โรงเรียนนายร้อยพระจุลจอมเกล้า . “หลักสูตรโรงเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า พ.ศ. 2562” . (ออนไลน์). เข้าถึงได้จาก : http://www.crma.ac.th/edu/EDU.pdf

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน) (สรอ.) . “ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)” . (ออนไลน์) . เข้าถึงได้จาก : https://www.dga.or.th/upload/download/file_769c60982e4c374dcd33b41c29227a31.pdf

## ภาษาต่างประเทศ

### Book

Darrill Gibson.ComTIA Security+ Get Cetified Get Ahead SYO-501 Study Guide. Printed in the United States of America , 2017.

# ภาคผนวก

# ผนวก ก
# แบบสอบถามการวิจัย

## แบบสอบถามการวิจัยเรื่อง
## “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562”

แบบสอบถามชุดนี้เป็นงานวิจัยเพื่อสำรวจความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อยโรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 เพื่อประกอบการทำวิจัยส่วนบุคคลของ พลตรี เอกรัตน์ ช้างแก้ว นักศึกษาวิทยาลัยป้องกันราชอาณาจักรรุ่นที่ 62 ประจำปี 2562

ดังนั้นจึงขอความร่วมมือจากนักเรียนกรุณาตอบแบบสอบถามให้สมบูรณ์ ข้อมูลทั้งหมดที่ตอบมาจะเป็นประโยชน์อย่างยิ่งสำหรับงานวิจัยครั้งนี้ การตอบแบบสอบถามจะไม่มีผลกระทบต่อนักเรียนแต่อย่างใด และขอขอบคุณที่ให้ความร่วมมือในการตอบแบบสอบถามครั้งนี้

**ตอนที่ 1** ข้อมูลทั่วไปของผู้ตอบแบบสอบถาม

**คำแนะนำ** : กรุณาตอบแบบสอบถาม โดยเลือกตัวเลือกที่ตรงกับท่านที่สุด

1. ปัจจุบันนักเรียนศึกษาที่โรงเรียนนายร้อยพระจุลจอมเกล้าอยู่ในชั้นปีใด
   - ○ ชั้นปีที่ 1
   - ○ ชั้นปีที่ 2
   - ○ ชั้นปีที่ 3
   - ○ ชั้นปีที่ 4
   - ○ ชั้นปีที่ 5
2. นักเรียนศึกษาหลักสูตรใดของโรงเรียนนายร้อยพระจุลจอมเกล้า
   (สำหรับนักเรียนชั้นปีที่ 1 ให้เลือกหลักสูตรที่มีความประสงค์จะเรียน)
   - ○ หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล
   - ○ หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมไฟฟ้าสื่อสาร
   - ○ หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมอุตสาหการ
   - ○ หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมโยธา
   - ○ หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมแผนที่
   - ○ หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์
   - ○ หลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี
   - ○ หลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา

**ตอนที่ 2** ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ จำนวน 10 ข้อ
**คำแนะนำ** : กรุณาตอบแบบสอบถาม โดยเลือกตัวเลือกที่ตรงกับตัวท่านที่สุด

| ลำดับ | เหตุการณ์ | เคย | ไม่เคย |
|---|---|---|---|
| 1 | นักเรียนเคยได้รับผลกระทบจากไวรัสที่ทำให้ไฟล์หรือโปรแกรมคอมพิวเตอร์เกิดความเสียหาย | | |
| 2 | นักเรียนเคยถูกการก่อกวนในระบบเครือข่ายทำให้ไม่สามารถทำงานได้อย่างมีประสิทธิภาพ | | |
| 3 | นักเรียนเคยติดตั้งโปรแกรมที่คิดว่าปลอดภัย แต่มีโปรแกรมอันตรายแฝงตัวเข้ามา | | |
| 4 | นักเรียนเคยถูกผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของนักเรียนได้โดยไม่รู้ตัว | | |
| 5 | นักเรียนถูกแอบดูพฤติกรรมหรือบันทึกการเข้าใช้งานคอมพิวเตอร์ | | |
| 6 | นักเรียนเคยโดนขโมยข้อมูลส่วนตัว เช่น บัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน | | |
| 7 | นักเรียนไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นจะได้รับข้อความ “เรียกค่าไถ่” | | |
| 8 | นักเรียนเคยถูกหลอกให้เข้าเว็บไซต์ปลอมเพื่อกรอกข้อมูลหรือเข้าระบบ | | |
| 9 | นักเรียนเคยได้รับจดหมายอิเล็กทรอนิกส์หลอกลวง | | |
| 10 | นักเรียนเคยได้รับโฆษณาที่ไม่พึงประสงค์จะได้รับ | | |

**ตอนที่ 3** ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ แบ่งเป็น 3 ด้าน คือ ความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการจารกรรมข้อมูล, ความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้าย และความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม

**คำแนะนำ** : กรุณาตอบแบบสอบถาม โดยเลือกตัวเลือกที่ตรงกับคำตอบ และความคิดเห็นของท่านที่สุด

3.1) ความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการจารกรรมข้อมูล

| ลำดับ | เหตุการณ์ | ไม่เคย | น้อย | ปานกลาง | มาก | มากที่สุด |
|---|---|---|---|---|---|---|
| 1 | นักเรียนตั้งรหัสผ่านมากกว่า 8 ตัวอักษรขึ้นไปหรือไม่ และนักเรียนตั้งรหัสผ่านที่ประกอบด้วย ตัวอักษรตัวเล็ก (Lowercase Letter) ตัวใหญ่ (Uppercase Letter) ตัวเลข (Number) และอักษรพิเศษ (Special Letter ต.ย.เช่น @,$,&,฿ เป็นต้น) หรือไม่ | | | | | |
| 2 | นักเรียนจดรหัสผ่านไว้ในที่ๆ นักเรียนสามารถเรียกดูได้หรือไม่ เช่น ในกระดาษ หรือ ในโทรศัพท์มือถือ | | | | | |
| 3 | นักเรียนใช้รหัสผ่านเดียวกันในทุกโปรแกรมหรือไม่ | | | | | |
| 4 | นักเรียนเปลี่ยนรหัสผ่านบ่อยหรือไม่ | | | | | |
| 5 | นักเรียนโพสต์ข้อมูลส่วนตัว เช่น ชื่อ นามสกุล ที่อยู่ เบอร์โทรศัพท์ วันเดือนปีเกิด บนสื่อสังคมออนไลน์หรือไม่ | | | | | |
| 6 | นักเรียนใช้ Wifi สาธารณะในการเปิดดูข้อมูลส่วนตัวหรือข้อมูลที่มีความสำคัญ เช่น ข้อมูลทางการเงินหรือไม่ | | | | | |
| 7 | นักเรียนออกจากระบบ (Log out) ทุกครั้งที่ใช้งานโปรแกรมหรือไม่ | | | | | |
| 8 | เมื่อเข้าเว็บไซต์ นักเรียนเลือก “Keep me logged in” หรือ “Remember me” หรือไม่ | | | | | |
| 9 | การทำธุรกรรมทางการเงินบนอินเทอร์เน็ต นักเรียนได้ตรวจสอบ URL ของเว็บไซต์ว่าเริ่มด้วย https:// หรือไม่ | | | | | |
| 10 | หากธนาคารที่นักเรียนใช้บริการอยู่เป็นประจำได้ส่งจดหมายอิเล็กทรอนิกส์ (E-mail) มายังนักเรียนเพื่อแจ้งการปรับปรุงระบบรักษาความปลอดภัยระหว่างนักเรียนและธนาคารให้ดียิ่งขึ้น โดยให้นักเรียนเข้าระบบ (Login) ด้วยการกรอกข้อมูลผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อดำเนินการกรอกข้อมูลในการปรับปรุงระบบ นักเรียนจะดำเนินการหรือไม่ | | | | | |

3.2) ความตระหนักรู้ภัยคุกคามไซเบอร์จากโปรแกรมประสงค์ร้าย

| ลำดับ | เหตุการณ์ | ไม่เคย | น้อย | ปานกลาง | มาก | มากที่สุด |
|---|---|---|---|---|---|---|
| 1 | นักเรียนจะดาวน์โหลดโปรแกรมฟรีบนอินเทอร์เน็ตมาติดตั้งบนเครื่องคอมพิวเตอร์ | | | | | |
| 2 | นักเรียนติดตั้งโปรแกรมป้องกันไวรัสที่ระบบคอมพิวเตอร์หรือไม่ | | | | | |
| 3 | นักเรียนอัพเดตโปรแกรม, แอพพลิเคชั่น อย่างสม่ำเสมอหรือไม่ | | | | | |
| 4 | ก่อนใช้งานอุปกรณ์สำรองข้อมูล นักเรียนทำการสแกนไวรัสทุกครั้งหรือไม่ | | | | | |
| 5 | หากนักเรียนบังเอิญพบอุปกรณ์อิเล็กทรอนิกส์ เช่น ทรัมป์ไดรฟ์ หรือ External Hard Disk ซึ่งไม่ทราบว่าเป็นของผู้ใด นักเรียนจะนำอุปกรณ์เหล่านี้ไปเปิดดูบนเครื่องคอมพิวเตอร์หรือไม่ | | | | | |
| 6 | นักเรียนเปิดไฟล์แนบ (Attachment) ในจดหมายอิเล็กทรอนิกส์ (E-mail) จากผู้ที่ไม่รู้จัก หรือไม่ทราบแหล่งที่มาหรือไม่ | | | | | |
| 7 | นักเรียนคลิกไปยังลิงค์ (Link) ของผู้ไม่รู้จักหรือไม่รู้จักแหล่งที่มาหรือไม่ | | | | | |
| 8 | นักเรียนสังเกตการทำงานของเครื่องคอมพิวเตอร์เสมอ เช่น การทำงานที่ช้าลง การรับ-ส่งข้อมูลที่ช้าลง และตรวจสอบว่ามีความผิดปกติหรือไม่ | | | | | |
| 9 | นักเรียนมีการสำรองข้อมูลสำคัญให้พอเพียงพร้อมใช้งานอยู่เสมอหรือไม่ | | | | | |
| 10 | นักเรียนกดดู โฆษณา เมื่อขึ้นมาบนจอคอมพิวเตอร์ (Pop-up Ads) หรือไม่ | | | | | |

3.3) ความตระหนักรู้ภัยคุกคามทางไซเบอร์ จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม

| ลำดับ | เหตุการณ์ | ไม่เคย | น้อย | ปานกลาง | มาก | มากที่สุด |
|---|---|---|---|---|---|---|
| 1 | เมื่อได้รับจดหมายลูกโซ่ หรือข้อมูลข่าวสาร นักเรียนส่งต่อหรือทำการแชร์ข้อมูลโดยไม่มีการตรวจสอบความถูกต้องหรือไม่ | | | | | |
| 2 | หากนักเรียนเชื่อหรือปฏิบัติตามข้อมูลบนสื่อออนไลน์ นักเรียนได้ทำการหาข้อมูล วิเคราะห์ และสรุปผลหาความถูกต้องก่อนที่จะเชื่อหรือปฏิบัติตามหรือไม่ | | | | | |
| 3 | นักเรียนนำภาพหรือข้อมูลของผู้อื่นที่ได้จากการคัดลอก (copy) หรือ ดาวน์โหลด (Download) โดยไม่ได้รับอนุญาตมาโพสต์โดยไม่ได้ให้เครดิตเจ้าของภาพหรือไม่ | | | | | |
| 4 | นักเรียนเคยกล่าวถึงผู้อื่นให้ได้รับความอับอายเสื่อมเสียชื่อเสียงผ่านทางไซเบอร์หรือไม่ | | | | | |
| 5 | นักเรียนเคยใช้ข้อความที่หยาบคายด่าว่าผู้อื่นผ่านทางไซเบอร์หรือไม่ | | | | | |
| 6 | นักเรียนเคยล้อเลียนรูปร่างหน้าตาของผู้อื่นผ่านทางไซเบอร์หรือไม่ | | | | | |
| 7 | นักเรียนเคยเผยแพร่ข่าวลือในทางลบของผู้อื่นผ่านทางไซเบอร์หรือไม่ | | | | | |
| 8 | นักเรียนเคยนำข้อมูลส่วนบุคคลของผู้อื่นไปเผยแพร่ผ่านทางไซเบอร์หรือไม่ | | | | | |
| 9 | นักเรียนเคยลบรายชื่อบุคคลที่ไม่ชอบออกจากกลุ่มสนทนาทางไซเบอร์หรือไม่ | | | | | |
| 10 | นักเรียนเคยกดดันให้บุคคลที่ไม่ชอบให้ออกจากกลุ่มสนทนาทางไซเบอร์หรือไม่ | | | | | |

# ผนวก ข
# ข้อมูลการสัมภาษณ์

จากการสัมภาษณ์นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าในเรื่องเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์นั้น ได้มีการแสดงความคิดเห็นเกี่ยวกับภัยคุกคามทางไซเบอร์และแนวทางการป้องกันดังนี้

1. ในปัจจุบันผมคิดว่าสื่อสังคมออนไลน์ มีความไวมาก ข่าวสารต่าง ๆ รับรู้กันได้อย่างรวดเร็ว และบางครั้งผู้ใช้สื่อสังคมออนไลน์ขาดความยั้งคิดก่อนที่จะสิ่งต่าง ๆ บนสื่อสังคมออนไลน์ ทำให้เกิดผลเสียตามมาได้ ฉะนั้น เราควรที่จะระมัดระวังในการใช้สื่อคิดและวิเคราะห์ให้ดีก่อนจะเผยแพร่หรือไม่ การรักษาความปลอดภัยที่เกี่ยวกับตัวเอง ในยุคนี้การเข้าถึงข้อมูลส่วนตัวของเราเป็นไปได้ง่ายมากซึ่งจะเกิดผลเสียกับตัวเราได้ ดังนั้นข้อมูลส่วนตัวต่าง ๆ ไม่ควรที่จะให้อยู่บนสื่อมากนักรวมไปถึงข้อมูลที่ความสำคัญต่าง ๆ ควรเก็บไว้ในพื้นที่ที่มีความปลอดภัย

2. การรักษาความปลอดภัยทางไซเบอร์ในระดับนักเรียนที่สามารถทำได้คือ เริ่มจากการที่รู้จักระมัดระวังในการกรอกข้อมูลส่วนตัวต่าง ๆ ลงในโลกออนไลน์ ต้องทำการตรวจสอบให้รอบคอบและถี่ถ้วนก่อน ในการใช้สื่อสังคมออนไลน์ควรเลือกใช้สื่อที่มีความน่าเชื่อถือ เป็นที่ยอมรับในด้านการรักษาความปลอดภัย และในการติดต่อสื่อสารกับบุคคลอื่นก็ไม่ควรที่จะเปิดเผยข้อมูลที่เป็นความลับหรือที่เป็นส่วนตัวมากจนเกินไป ถ้าหากไม่มั่นใจหรือสงสัยเกี่ยวกับการใช้สื่อสังคมออนไลน์อย่างไรให้ปลอดภัย ให้ปรึกษาผู้ที่มีประสบการณ์ นำความรู้ต่าง ๆ ไปสอน ไปอบรมให้แก่ผู้ที่มีปัญหาหรือผู้ทีเริ่มใช้สื่อออนไลน์

3. ควรมีการสอนการใช้งาน การป้องกันต่าง ๆ เช่น เทคนิคในการตรวจสอบว่าอุปกรณ์ของเรามีการถูกแฮคหรือไม่ วิธีตรวจสอบ URL ว่าถูกต้องไม่ผิดปกติ มีการจัดผู้เชี่ยวชาญจากแหล่งชั้นนำมาสอนถึงข้อดี ข้อเสียให้กับนักเรียนทุกส่วน คือสอนในรายละเอียดทั้งพื้นฐาน สิ่งที่ควรรู้ สิ่งที่สามารถพบได้ในชีวิตประจำวัน การระวังตัวจากการเข้าเว็บไซต์ต่าง ๆ ด้วย

4. ในอาชีพทหารต้องให้ความสำคัญกับการรักษาความลับของทางราชการ จึงควรมีมาตรการในการเปิดเผยหรือเผยแพร่ข้อมูลส่วนตัวของกำลังพล การเข้าถึงข้อมูลของหน่วยงานในกองทัพต่าง ๆ โดยเฉพาะอย่างยิ่งในปัจจุบัน การได้เปรียบในการรบขึ้นอยู่กับการรับรู้ข้อมูลข่าวสารของศัตรูซึ่งอยู่ในรูปแบบของไซเบอร์

5. ควรมีการจัดการส่งเสริมความรู้ทางด้านการรักษาความปลอดภัยทางไซเบอร์ให้มากขึ้น เนื่องจากในปัจจุบันมีสื่อออนไลน์มากมายที่ความปลอดภัยและไม่ปลอดภัย เราจึงควรส่งเสริมให้ผู้ที่ใช้สื่อสังคมออนไลน์ใช้สื่อสังคมออนไลน์ได้อย่างถูกต้อง และปลอดภัยจากมิจฉาชีพทาออนไลน์ เพราะในปัจจุบันเทคโนโลยีได้พัฒนาไปไกลมาก จึงเป็นอันง่ายที่จะทำการขโมยข้อมูลทางสื่อสังคมออนไลน์

6. ไม่รับเพื่อนผู้ติดตามที่เราไม่รู้จัก พยายามอย่าเปิดเผยข้อมูลสำคัญถ้าไม่จำเป็น มีสติสัมปชัญญะ อย่าหลงเชื่อโฆษณาการเล่นรับของรางวัลต่าง ๆ ที่ไม่สมเหตุสมผล ไม่ควรหมกมุ่นมากจนเกินไป ตั้งรหัสรักษาความปลอดภัยที่คาดเดาได้ยาก มีรหัสสำรองเมื่อถูกคุกคาม ในปัจจุบันทุกคนสนใจและใช้สื่อสังคมออนไลน์เป็นส่วนมาก จึงควรรักษาความปลอดภัยส่วนตัวของตัวเองให้ดี

-

# ประวัติย่อผู้วิจัย

**ชื่อ** พลตรี เอกรัตน์ ช้างแก้ว

**วัน เดือน ปี เกิด** 25 ตุลาคม 2507

**การศึกษา** วิทยาศาสตรบัณฑิต สาขาเครื่องกล
โรงเรียนนายร้อยพระจุลจอมเกล้า
รัฐศาสตรมหาบัณฑิต สาขาความสัมพันธ์ระหว่างประเทศ
มหาวิทยาลัยธรรมศาสตร์
ศิลปศาสตรมหาบัณฑิต สาขาวิชาภาษาอังกฤษเพื่ออาชีพ
มหาวิทยาลัยธรรมศาสตร์
ศิลปศาสตรมหาบัณฑิต สาขาวิชาการแปลอังกฤษและไทย
มหาวิทยาลัยธรรมศาสตร์

**ประวัติการทำงาน**

ตำแหน่งรับราชการ

ผู้บังคับกองร้อยอาวุธเบา กองพันทหารราบที่ 3 กรมทหารราบที่ 1
มหาดเล็กรักษาพระองค์
ผู้บังคับกองพันทหารราบที่ 3 กรมทหารราบที่ 1 มหาดเล็กรักษาพระองค์
ผู้บังคับการกรมทหารราบที่ 1 มหาดเล็กรักษาพระองค์
รองผู้บัญชาการกองพลที่ 1 รักษาพระองค์
เสนาธิการ กองทัพน้อยที่ 1
รองผู้บัญชาการ โรงเรียนนายร้อยพระจุลจอมเกล้า

ราชการพิเศษ หัวหน้าฝ่ายกำลังพล กองกำลังทหารบกไทย/ติมอร์
หัวหน้าฝ่ายกำลังพล กองกำลัง 972 ไทย/ติมอร์ตะวันออก
หัวหน้าคณะนายทหารไทยประจำ บก.สหประชาชาติ ณ ชายแดน
อิรัค - คูเวต
ผู้บังคับหน่วยเฉพาะกิจนราธิวาส
เลขาธิการ กอ.รมน.ภาค 1

**ตำแหน่งปัจจุบัน** รองผู้บัญชาการ โรงเรียนนายร้อยพระจุลจอมเกล้า

# สรุปย่อ

**ลักษณะวิชา** วิทยาศาสตร์ เทคโนโลยี พลังงาน และสิ่งแวดล้อม
**เรื่อง** ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562
**ผู้วิจัย** พลตรี เอกรัตน์ ช้างแก้ว **หลักสูตร** วปอ. **รุ่นที่** 62
**ตำแหน่ง** รองผู้บัญชาการโรงเรียนนายร้อยพระจุลจอมเกล้า

---

## ความเป็นมาและความสำคัญของปัญหา

วิทยาการด้านเทคโนโลยีสารสนเทศและการสื่อสารก้าวหน้าไปอย่างรวดเร็วในช่วง 10 ปีที่ผ่านมาและยังพัฒนาต่อไปในรูปแบบที่หลากหลายมากขึ้น มีการกระจายไปในทุกระบบของสังคม นำมาซึ่งความสะดวกสบายของผู้คนบนโลกที่เข้าถึงและนำมาประยุกต์เพื่อใช้ประโยชน์กับตนเองและกับสังคม เศรษฐกิจ การเมือง ความมั่นคง แต่อย่างไรก็ตามความก้าวหน้าและการพัฒนาทางด้านเทคโนโลยีเหล่านี้ก็อาจนำมาซึ่งภัยอันตรายขนาดเล็กระดับบุคคล ครอบครัว องค์กรจนถึงขนาดใหญ่ระดับประเทศหรือระดับโลกได้ ซึ่งรูปแบบของภัยอันตรายที่เปลี่ยนแปลงไปจากเดิมนี้ เรียกว่าภัยคุกคามทางไซเบอร์ (Cyber Threats)

ปัจจุบันหน่วยงานต่าง ๆ ได้พยายามป้องกันภัยคุกคามทางไซเบอร์นี้ โดยให้ความสำคัญในการพัฒนาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) มากขึ้น อาจเพราะเห็นผลร้ายที่เกิดขึ้นทั้งในองค์กรเอง และตัวอย่างจากนอกองค์กรที่เป็นข่าวอยู่บ่อยครั้งหรือด้วยกฎหมายบังคับให้ต้องปฏิบัติตาม ทำให้มีการพัฒนาเรื่องดังกล่าวไปพอสมควร แต่อย่างไรก็ตามยังต้องมีเรื่องที่ต้องทำความเข้าใจและปรับปรุงให้ดีขึ้นอีกมาก เพื่อให้เท่าทันไปกับรูปแบบของภัยคุกคามที่เปลี่ยนแปลงไป

สิ่งหนึ่งที่ต้องให้ความสำคัญคือการพัฒนาศักยภาพของบุคลากรในองค์กร ให้มีความเข้าใจในการบริหารจัดการและการใช้เครื่องมือต่าง ๆ ได้อย่างมีประสิทธิภาพและเป็นไปตามกระบวนการที่เหมาะสม เพราะถ้านำมาใช้ไม่ถูกต้อง ไม่มีความเข้าใจก็จะเสียทั้งงบประมาณและความคุ้มค่าในการดำเนินการ ซึ่งการจะทำความเข้าใจสิ่งเหล่านี้นั้น ต้องมีพื้นฐานความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ เพื่อนำไปประยุกต์ใช้เทคโนโลยีด้านสารสนเทศต่าง ๆ ได้อย่างเหมาะสม ให้เกิดความมั่นคงปลอดภัยทางไซเบอร์ ป้องกันความเสียหายต่าง ๆ ที่อาจเกิดขึ้นกับองค์กรได้

โรงเรียนนายร้อยพระจุลจอมเกล้า เป็นหน่วยงานหลักที่ผลิตนายทหารสัญญาบัตรหลักให้กับกองทัพบก ผู้บังคับบัญชาของกองทัพบกจึงเล็งเห็นความสำคัญในการพัฒนานักเรียนนายร้อยให้มีความรู้ ความสามารถด้านไซเบอร์และการรักษาความปลอดภัยทางไซเบอร์ ให้เท่าทันเทคโนโลยีในปัจจุบัน แต่การจะพัฒนาความรู้ด้านไซเบอร์ให้กับนักเรียนนายร้อยได้ จำเป็นต้องทราบพื้นฐานความตระหนักรู้ด้านภัยคุกคามทางด้านไซเบอร์ก่อน เพื่อเป็นแนวทางในการพัฒนาต่อยอดองค์ความรู้ให้กับนักเรียนนายร้อยได้อย่างเหมาะสม ผู้วิจัยจึงได้วิจัยเรื่องความตระหนักรู้ภัยคุกคามทางไซเบอร์

ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า เพื่อเป็นการศึกษาพื้นฐานด้านบุคลากรของนายทหารสัญญาบัตรหลักของกองทัพบกในอนาคต ว่ามีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์มากน้อยเพียงใด และมีความพร้อมที่จะรับมือกับภัยคุกคามทางไซเบอร์ ได้พอเพียงหรือไม่ โดยในอนาคตสามารถนำไปใช้ทบทวนในการพิจารณาพัฒนาหลักสูตรความปลอดภัยทางไซเบอร์ให้กับนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ได้อย่างเหมาะสมและมีประสิทธิภาพ เพื่อให้เป็นนายทหารที่มีบทบาทสำคัญในเผยแพร่ความรู้ให้กับกำลังพลในกองทัพ การระวังป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของตนเอง และของหน่วยงานของกองทัพบก และมีศักยภาพในการส่งเสริมความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพบกและประเทศชาติต่อไป

## วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาความเข้าใจภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 และแนวทางการรักษาความปลอดภัยทางไซเบอร์ในปัจจุบัน
2. เพื่อวิเคราะห์ประเมินความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า
3. เพื่อเสนอแนวทางการพัฒนาหลักสูตรการรักษาความปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ
4. เพื่อเสนอการประยุกต์ใช้ในการพัฒนาบุคลากรของกองทัพบกในการรับมือกับภัยคุกคามทางไซเบอร์ต่อไป

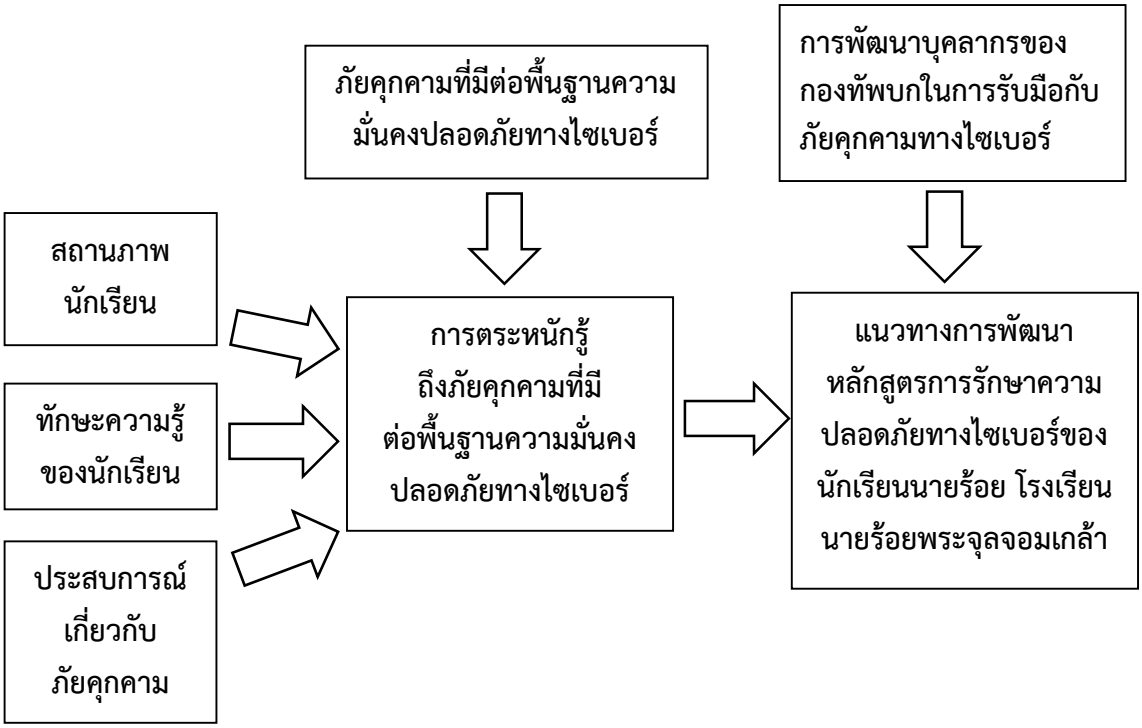
## ขอบเขตการวิจัย

1. ประชากร นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ที่กำลังศึกษาในปีการศึกษา 2562 จำนวน 1,184 นาย
2. กลุ่มตัวอย่าง นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ชั้นปีที่ 1- 5 ที่กำลังศึกษาในภาคการศึกษาที่ 2 ปีการศึกษา 2562 จำนวน 300 นาย
3. ตัวแปรที่ใช้
    - 3.1 ตัวแปรต้น
        - 3.1.1 ชั้นปีของนักเรียนนายร้อย
        - 3.1.2 หลักสูตรที่ศึกษา
        - 3.1.3 ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์
    - 3.2 ตัวแปรตาม ความตระหนักรู้ภัยคุกคามทางไซเบอร์
        - 3.2.1 การจารกรรมข้อมูล
        - 3.2.2 โปรแกรมประสงค์ร้าย
        - 3.2.3 สื่อสังคมออนไลน์ที่ไม่เหมาะสม

4. เอกสารวิจัยฉบับนี้ เป็นการวิจัยเชิงปริมาณและเชิงคุณภาพหรือแบบผสมผสาน (Mixed Method) โดยการทำแบบสอบถามที่ให้ความสำคัญกับมุมมอง ประสบการณ์ และการกระทำของกลุ่มที่ต้องการศึกษาและนำมาวิเคราะห์เพื่อให้เข้าใจความตระหนักรู้ด้านไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

## กรอบแนวคิดการวิจัย

ผู้วิจัยกำหนดกรอบแนวคิดในการศึกษาหัวข้อ “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” ดังนี้




## ทบทวนวรรณกรรมที่เกี่ยวข้อง

การศึกษาเรื่อง “ความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562” ผู้วิจัยได้รวบรวมแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องที่ต้องการศึกษา โดยแนวคิด ทฤษฎี วรรณกรรม และงานวิจัยที่เกี่ยวข้องที่รวบรวมมี ดังนี้

1. แนวคิดและทฤษฎีที่เกี่ยวข้องกับความรู้ ทัศนคติ และพฤติกรรม
2. แนวความคิดเกี่ยวกับความตระหนักรู้
3. แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)
4. รูปแบบการรักษาความปลอดภัยทางไซเบอร์
5. ทฤษฎีเกี่ยวกับภัยคุกคามทางไซเบอร์ (Cyber Threats)

6. นโยบายและแผนระดับชาติว่าด้วยความมั่นคงแห่งชาติ (พ.ศ. 2562 - 2565)

7. ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (พ.ศ. 2560 - 2564)

8. การพัฒนาบุคลากรของกองทัพบกในการรับมือกับภัยคุกคามทางไซเบอร์

9. มาตรฐานการรักษาความปลอดภัยทางไซเบอร์ในระดับสากล

10. หลักสูตรของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562

11. พันธกิจของโรงเรียนนายร้อยพระจุลจอมเกล้าในการผลิตนายทหารสัญญาบัตร

12. การพัฒนาหลักสูตรการรักษาปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

13. งานวิจัยที่เกี่ยวข้อง

## การออกแบบการวิจัย

การดำเนินการวิจัยครั้งนี้ใช้วิธีวิทยาการวิจัยแบบผสม (Mixed Method) ประกอบด้วย การวิจัยเชิงปริมาณ (Quantitative Research) และการวิจัยเชิงคุณภาพ (Qualitative Research) โดยใช้การวิจัยเชิงปริมาณ เพื่อศึกษาปัจจัยความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 และใช้การวิจัยเชิงคุณภาพเพื่อศึกษาปัญหาและแนวทางในการพัฒนาการสร้างความตระหนักรู้ภัยคุกคามทางไซเบอร์ให้กับนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า

## ประชากรและกลุ่มตัวอย่าง

การประเมินความตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ปีการศึกษา 2562 มีประชากร จำนวน 1,184 นาย ผู้วิจัยกำหนดค่าคลาดเคลื่อนของการเลือกกลุ่มตัวอย่างหรือค่าคลาดเคลื่อนของการประเมินค่าไว้ที่ร้อยละ 5 หรือ 0.05 ดังนั้นจะใช้กลุ่มตัวอย่างดังนี้

แทนค่าในสูตร $n = N/1+Ne^2$

จะได้ $n = 1184/1+(1184 * 0.05^2)$ $n = 298.9899$

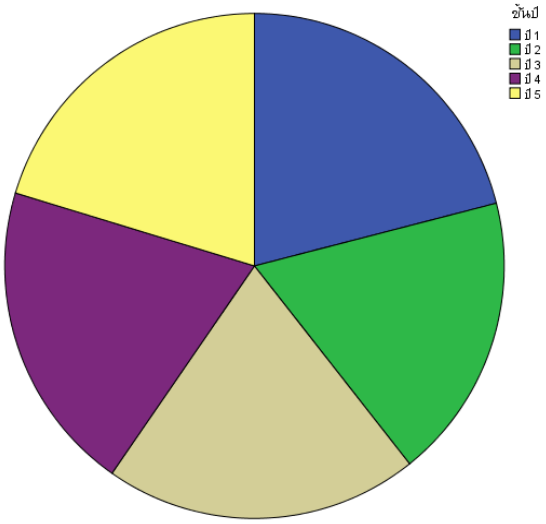
จากการคำนวณจะได้ขนาดตัวอย่าง 298 นาย แต่ในการวิจัยครั้งนี้จะใช้ขนาดตัวอย่าง 300 นาย

## ผลการวิจัย

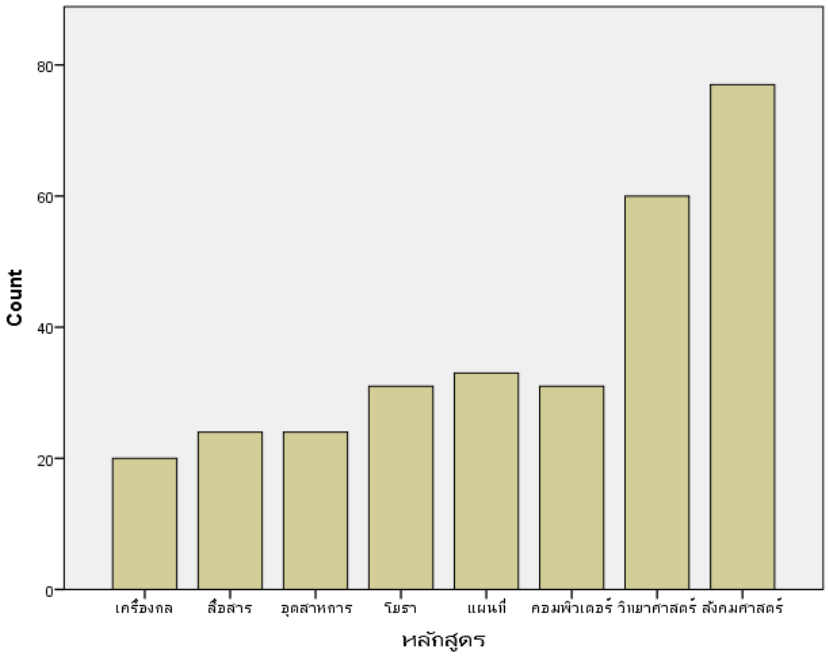
ผู้วิจัยได้ทำการวิเคราะห์ข้อมูลและได้เสนอการวิเคราะห์ข้อมูล ผลการวิจัย แบ่งเป็น 3 ตอน ดังนี้

1. ข้อมูลลักษณะของประชากร
2. ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์
3. ความตระหนักเกี่ยวกับภัยคุกคามทางไซเบอร์

## ข้อมูลลักษณะของประชากร

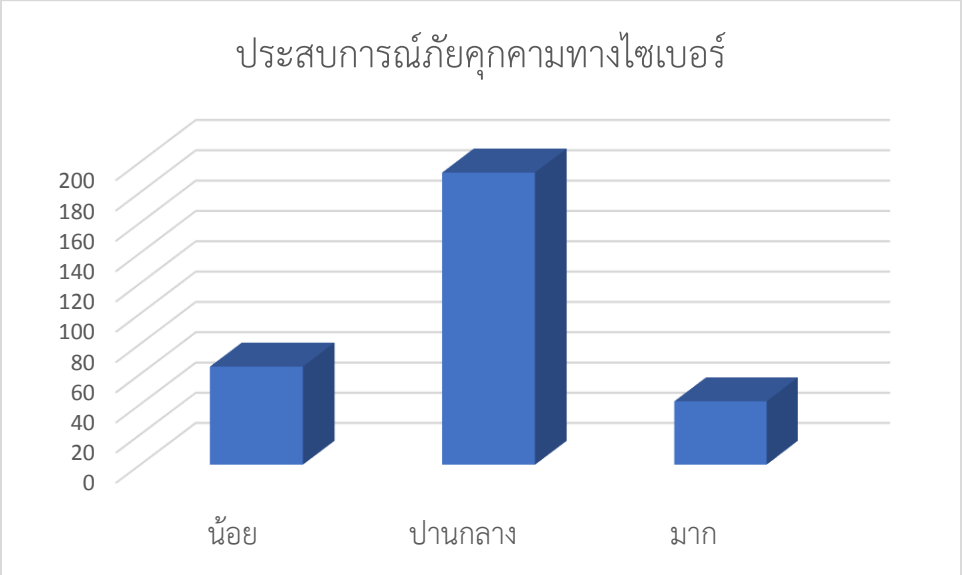



ผู้ตอบแบบสอบถามในแต่ละชั้นปี มีจำนวนใกล้เคียงกัน




ลักษณะประชากรของผู้ตอบแบบสอบถามในแต่ละหลักสูตร พบว่าผู้ตอบแบบสอบถามส่วนมากศึกษาหลักสูตรศิลปศาสตรบัณฑิต สาขาวิชาสังคมศาสตร์เพื่อการพัฒนา รองลงมาคือหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี หลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมแผนที่และวิศวกรรมศาสตรบัณฑิต สาขาวิชาวิศวกรรมเครื่องกล มีผู้ตอบแบบสอบถามน้อยที่สุด

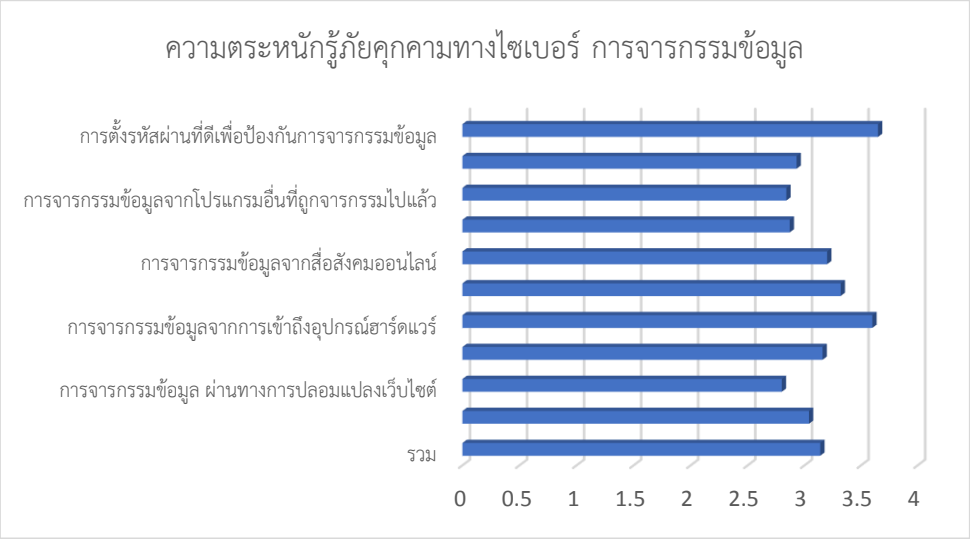
## ประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์




ผู้ที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ โดยแบ่งกลุ่มเป็นผู้มีประสบการณ์น้อย ปานกลางและมาก โดยผู้ที่มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์ส่วนใหญ่จะมีประสบการณ์อยู่ในระดับปานกลาง

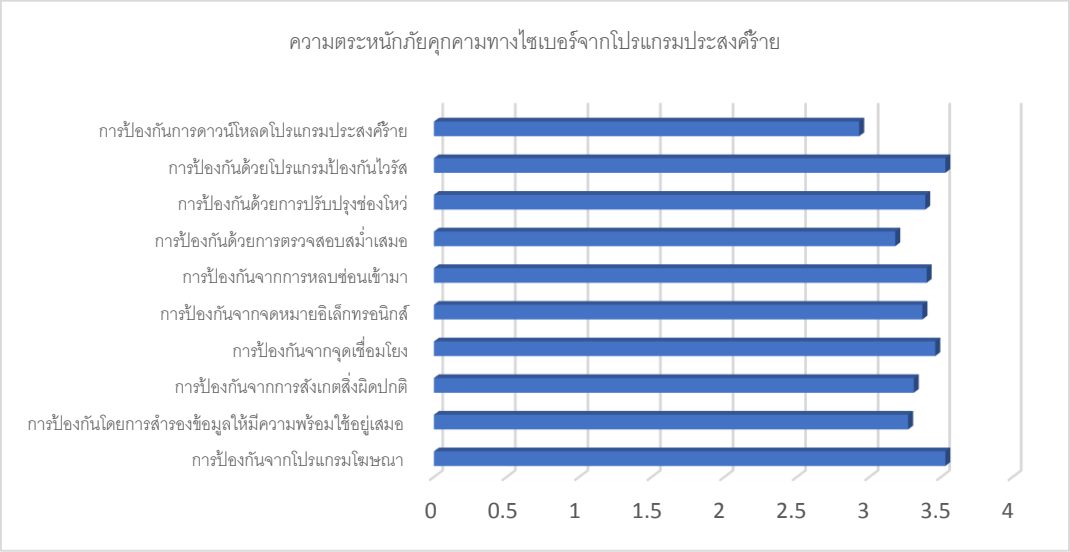
## ความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์

### ความตระหนักรู้ภัยคุกคามทางไซเบอร์ การจารกรรมข้อมูล



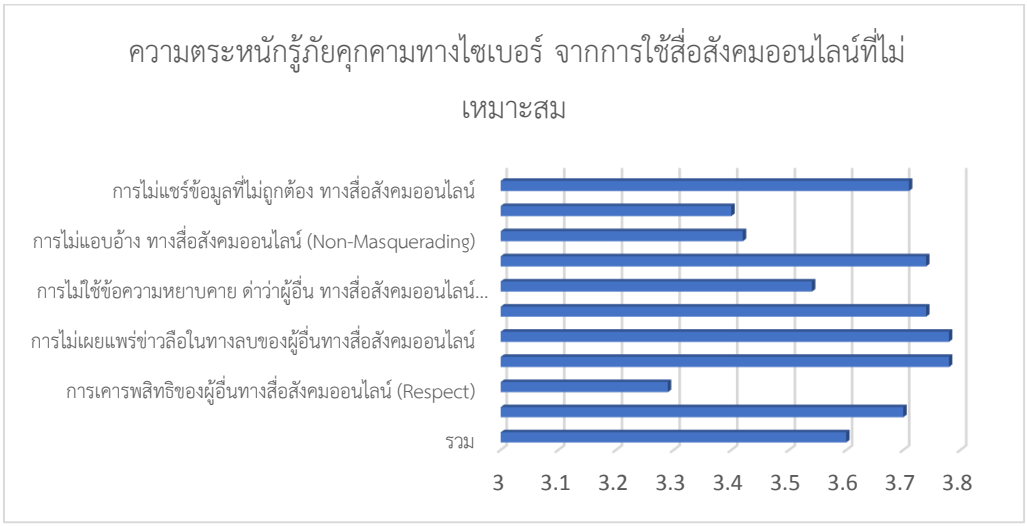
ผู้ตอบแบบสอบถาม มีความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการจารกรรมข้อมูลอยู่ในระดับปานกลาง โดยการป้องกันการจารกรรมข้อมูลที่กลุ่มตัวอย่างมีความตระหนักมากคือการตั้งรหัสผ่านที่ดีเพื่อป้องกันการจารกรรมข้อมูล และน้อยที่สุดคือการป้องกันการจารกรรมข้อมูลผ่านทางการปลอมแปลงเว็บไซต์

## ความตระหนักรู้ภัยคุกคามทางไซเบอร์ จากโปรแกรมประสงค์ร้าย




ผู้ตอบแบบสอบถาม มีความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้ายโดยรวมอยู่ในระดับปานกลาง โดยการป้องกันโปรแกรมประสงค์ร้ายที่กลุ่มตัวอย่างมีความตระหนักมากคือการป้องกันตนเองด้วยโปรแกรมป้องกันไวรัส และการป้องกันตนเองจากโปรแกรมโฆษณาและตระหนักน้อยที่สุดคือการป้องกันการดาวน์โหลดโปรแกรมประสงค์ร้าย

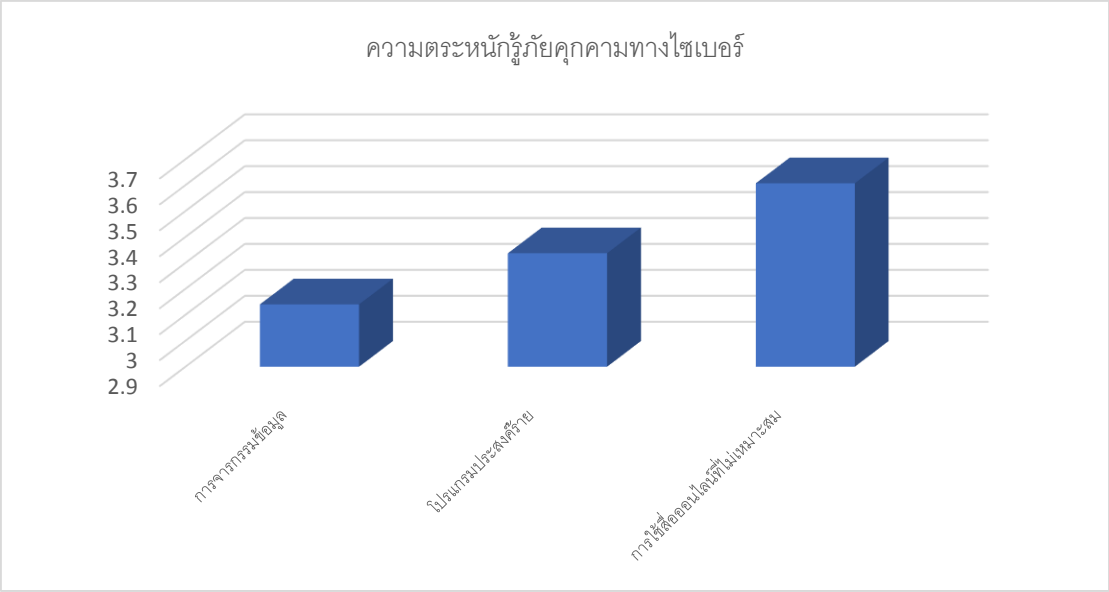
## ความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสม



ผู้ตอบแบบสอบถาม มีความตระหนักรู้ภัยคุกคามทางไซเบอร์จากการใช้สื่อสังคมออนไลน์ที่ไม่เหมาะสมโดยรวมอยู่ในระดับสูง โดยการใช้สื่อสังคมออนไลน์ที่กลุ่มตัวอย่างมีความตระหนักมากคือการไม่เผยแพร่ข่าวลือในทางลบของผู้อื่นทางสื่อสังคมออนไลน์ และการไม่เผยแพร่ข้อมูลส่วนบุคคลของผู้อื่นทางสื่อสังคมออนไลน์ การไม่ทำให้ผู้อื่นอับอายหรือเสียชื่อเสียงและความตระหนักน้อยที่สุดคือการเคารพสิทธิของผู้อื่นทางสื่อสังคมออนไลน์

**สรุปความตระหนักรู้ภัยคุกคามทางไซเบอร์ทุกด้าน (การจารกรรมข้อมูล, โปรแกรมประสงค์ร้าย, การใช้สื่อออนไลน์ที่ไม่เหมาะสม)**

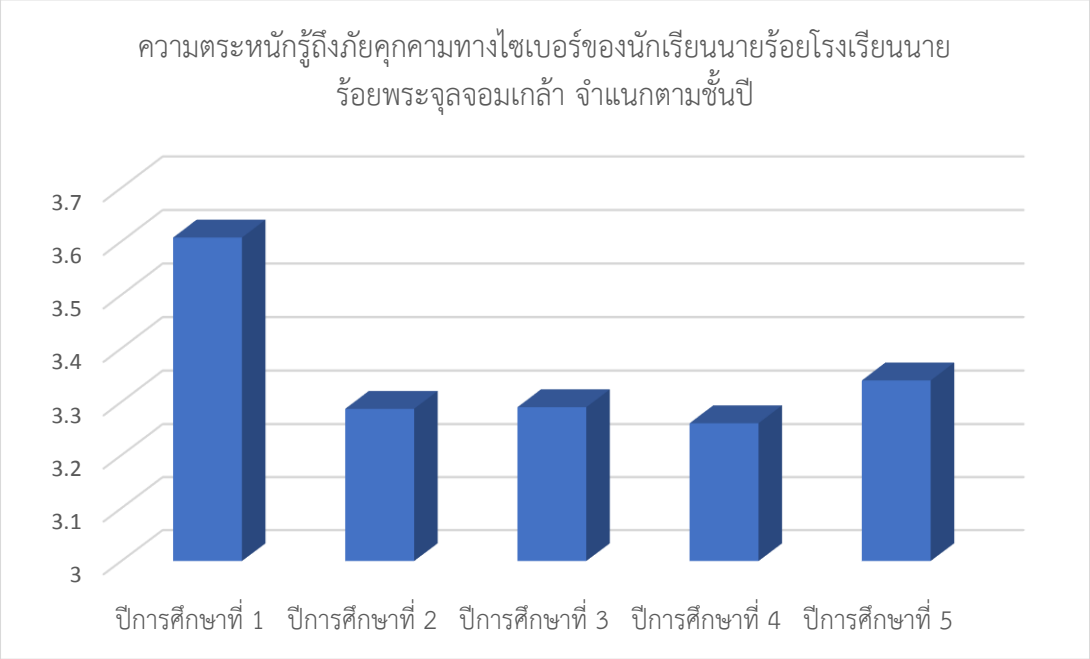
| ความตระหนักรู้ภัยคุกคามทางไซเบอร์ | | | | | | |
|---|---|---|---|---|---|---|
| ประเด็น | N | Min | Max | M | SD | ระดับ |
| การจารกรรมข้อมูล | 300 | 2.00 | 4.50 | 3.140 | 0.423 | ปานกลาง |
| โปรแกรมประสงค์ร้าย | 300 | 2.20 | 5.00 | 3.337 | 0.530 | ปานกลาง |
| การใช้สื่อออนไลน์ที่ไม่เหมาะสม | 300 | 1.80 | 5.00 | 3.607 | 0.795 | มาก |
| รวม | 300 | 2.40 | 4.83 | 3.361 | 0.469 | ปานกลาง |




พบว่า ผู้ตอบแบบสอบถามมีความตระหนักรู้ภัยคุกคามทางไซเบอร์การใช้สื่อออนไลน์ที่ไม่เหมาะสมอยู่ในระดับสูง (3.607) รองลงมาคือความตระหนักรู้ภัยคุกคามทางไซเบอร์จากโปรแกรมประสงค์ร้ายระดับปานกลาง (3.337) และความตระหนักรู้ภัยคุกคามทางไซเบอร์ด้านการจารกรรมข้อมูลระดับปานกลาง (3.14)

**ปัจจัยทางด้านชั้นปีการศึกษามีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า**

| ชั้นปีการศึกษา | N | M | SD | ระดับ |
|---|---|---|---|---|
| ปีการศึกษาที่ 1 | 63 | 3.607 | 0.548 | มาก |
| ปีการศึกษาที่ 2 | 55 | 3.287 | 0.399 | ปานกลาง |
| ปีการศึกษาที่ 3 | 61 | 3.292 | 0.466 | ปานกลาง |
| ปีการศึกษาที่ 4 | 60 | 3.262 | 0.474 | ปานกลาง |
| ปีการศึกษาที่ 5 | 61 | 3.340 | 0.350 | ปานกลาง |

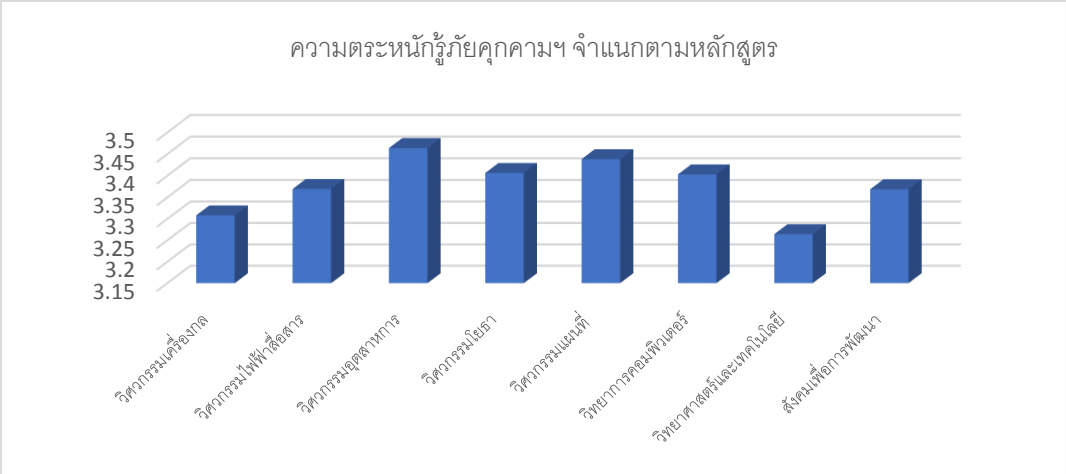



ความตระหนักรู้ภัยคุกคามทางไซเบอร์แยกตามชั้นปี พบว่านักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 1 มีความตระหนักรู้ในระดับสูงมีค่าเฉลี่ยมากที่สุด (3.607) และน้อยที่สุดคือ นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 4 (3.262)

**การวิเคราะห์ความแปรปรวนแบบทางเดียวของความตระหนักภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามชั้นปี**

พบว่า นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าชั้นปีที่ 1 จะมีความตระหนักรู้ภัยคุกคามทางไซเบอร์มากกว่าชั้นปีที่ 2 ชั้นปีที่ 3 ชั้นปีที่ 4 และ ชั้นปีที่ 5 อย่างมีนัยสำคัญ

**ปัจจัยด้านหลักสูตรการศึกษามีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า**




ความตระหนักรู้ภัยคุกคามทางไซเบอร์แยกตามหลักสูตร พบว่า นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า มีความตระหนักรู้ในระดับปานกลาง โดยหลักสูตรวิศวกรรมศาสตรบัณฑิต สาขาวิศวกรรมอุตสาหการ มีความตระหนักมากที่สุด และหลักสูตรวิทยาศาสตรบัณฑิต สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มีความตระหนักรู้น้อยที่สุด

**การวิเคราะห์ความแปรปรวนแบบทางเดียวของการตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามหลักสูตรการศึกษา**

พบว่า นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าในแต่ละหลักสูตรจะมีความตระหนักรู้ภัยคุกคามทางไซเบอร์อยู่ในระดับปานกลางไม่แตกต่างกัน

**ปัจจัยทางด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า**

การเปรียบเทียบความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามความตระหนักรู้ภัยคุกคามทางไซเบอร์

| ประสบการณ์ | Mean | N | SD. | ระดับ |
|---|---|---|---|---|
| น้อย | 3.5010 | 65 | .54661 | มาก |
| ปานกลาง | 3.3337 | 193 | .46450 | ปานกลาง |
| มาก | 3.2738 | 42 | .29991 | ปานกลาง |

การวิเคราะห์ความแปรปรวนแบบทางเดียวของการตระหนักรู้ภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า จำแนกตามประสบการณ์ภัยคุกคามทางไซเบอร์

| **แหล่งที่มา** | SS | Df | MS | F | P |
|---|---|---|---|---|---|
| ระหว่างกลุ่ม | 1.738 | 2 | 0869 | 4.017* | .019 |
| ภายในกลุ่ม | 64.237 | 297 | .216 | | |
| รวม | 65.974 | 299 | | | |

หมายเหตุ *** มีนัยสำคัญทางสถิติที่ระดับ 0.05

พบว่า นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าที่มีประสบการณ์ภัยคุกคามทางไซเบอร์น้อยจะมีความตระหนักรู้ภัยคุกคามทางไซเบอร์มากกว่านักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าที่มีประสบการณ์ภัยคุกคามทางไซเบอร์ระดับปานกลางและระดับสูง อย่างมีนัยสำคัญ

# สรุปผลการวิจัยและข้อเสนอแนะ

ปัจจัยด้านชั้นปีการศึกษา พบว่านักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า โดยรวมมีความตระหนักรู้ภัยคุกคามด้านไซเบอร์ค่าเฉลี่ยอยู่ในระดับปานกลาง สำหรับการแยกในแต่ละชั้นปี พบว่านักเรียนนายร้อยชั้นปีที่ 1 มีความตระหนักถึงภัยคุกคามทางไซเบอร์มากกว่านักเรียนชั้นปีอื่น ๆ อย่างมีนัยสำคัญ การระบุกลุ่มตัวอย่างได้ดังนี้ สามารถนำไปวิเคราะห์ความแตกต่างเรื่องอายุหรือชั้นปีการศึกษาเพื่อหาแนวทางกำหนดกลุ่มเป้าหมายและวิธีป้องกันในการลดความเสี่ยงจากภัยคุกคามของการโจมตีทางไซเบอร์ สร้างความตระหนักและความเข้าใจเพื่อลดผลกระทบที่อาจเกิดขึ้นจากการใช้งานและใช้ชีวิตประจำวัน

ปัจจัยด้านหลักสูตรการศึกษา พบว่าไม่มีผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า เนื่องจากนักเรียนนายร้อยที่ศึกษาในหลักสูตรที่แตกต่างกัน มีความตระหนักรู้ภัยคุกคามทางด้านไซเบอร์ในระดับปานกลางเช่นเดียวกัน ดังนี้ข้อมูลดังกล่าว สามารถนำไปสร้างแนวทางในการจัดการศึกษาอบรมเกี่ยวกับการสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์เพิ่มในแต่ละหลักสูตรได้ไม่ต่างกัน

ปัจจัยด้านประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์มีผลต่อความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า โดยจะเห็นได้ว่าผู้ที่มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์น้อยนั้น มีความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์มากอย่างมีนัยสำคัญ อาจแสดงให้เห็นว่ากลุ่มตัวอย่างที่มีความตระหนักรู้ถึงภัยคุกคามทางไซเบอร์จะคอยระวังป้องกันตนเองจากภัยต่าง ๆ ที่เกิดขึ้น ส่งผลให้มีประสบการณ์เกี่ยวกับภัยคุกคามทางไซเบอร์น้อย

ดังนั้น แนวทางในการจัดการศึกษาอบรมเกี่ยวกับความตระหนักถึงภัยคุกคามทางไซเบอร์ที่มีประสิทธิภาพ ให้นักเรียนนายร้อยมีความตระหนักรู้มากขึ้นก็จะช่วยป้องกันภัยคุกคามทางไซเบอร์ได้

## ข้อเสนอแนวทางการพัฒนาหลักสูตรวิทยาศาสตรบัณฑิต สาขาความมั่นคงปลอดภัยทางไซเบอร์

### 1. สอดคล้องกับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสากล

จากการกำเนิดของโลกาภิวัตน์ทำให้หลาย ๆ ระบบเกิดการเชื่อมโยงเข้าไว้ด้วยกัน ดังที่เห็นในปัจจุบัน เทคโนโลยีสารสนเทศทำให้โลกเชื่อมกันดังกล่าว ภัยคุกคามทางด้านไซเบอร์ก็สามารถเชื่อมโยงไปถึงกันหมดเช่นเดียวกัน การพัฒนาหลักสูตรวิทยาศาสตรบัณฑิต สาขาความมั่นคงปลอดภัยทางไซเบอร์ของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าจึงต้องสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสากล ซึ่งในปัจจุบันมีการจัดทำมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์เกิดขึ้นหลายองค์กร การพัฒนาหลักสูตรจึงควรมีการศึกษามาตรฐานต่าง ๆ และเลือกมาตรฐานที่เหมาะสมเพื่อใช้เป็นแนวทางในการกำหนดวิชาต่าง ๆ ในหลักสูตรเพื่อให้สอดคล้องกับมาตรฐานเหล่านั้นและมีการจัดทำคลังข้อสอบเพื่อเตรียมการให้นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าได้ศึกษาเพื่อเตรียมการสอบตามมาตรฐานของสากล รวมถึงการจัดหางบประมาณในการสอบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสากล และในอนาคตโรงเรียนนายร้อยพระจุลจอมเกล้า อาจสามารถพัฒนาเป็นสถาบันอีกแห่งหนึ่งที่ใช้ในการทดสอบมาตราฐานความปลอดภัยไซเบอร์ในระดับประเทศระดับอาเซียน หรือแม้แต่ระดับโลกได้

### 2. ความรู้พื้นฐานทางเทคโนโลยีสารสนเทศที่จำเป็น

การปรับปรุงหลักสูตรวิทยาศาสตรบัณฑิต สาขาความมั่นคงปลอดภัยทางไซเบอร์ในปัจจุบัน โรงเรียนนายร้อยพระจุลจอมเกล้า ได้ทำการปรับหลักสูตรมาจากหลักสูตรวิทยาศาสตร์บัณฑิตสาขาวิทยาการคอมพิวเตอร์ ซึ่งเดิมเป็นหลักสูตรหลักของนักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้า ซึ่งจะจบการศึกษาไปจะเป็นกำลังหลักในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศของกองทัพบก เมื่อมีการปรับปรุงหลักสูตรโดยการยกเลิกบางวิชา และนำวิชาการเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์เข้ามาเสริม ผู้วิจัยมีความเห็นว่าจะทำให้นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าที่จบหลักสูตรไม่ได้รับความรู้พื้นฐานทางเทคโนโลยีสารสนเทศที่ต้องใช้ในการทำงานในอนาคตที่เกี่ยวกับวิทยาการคอมพิวเตอร์เพียงพอ เพราะอย่างไรก็ตามกองทัพบกก็ยังมีความจำเป็นต้องใช้กำลังพลที่จบการศึกษาในหลักสูตรเหล่านี้ไปปฏิบัติหน้าที่ที่เกี่ยวข้องกับสายงานสารสนเทศของกองทัพบก และในปัจจุบันเทคโนโลยีสารสนเทศก็เข้าไปมีบทบาทในเกือบทุกสายงาน สำหรับวิชาที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่เสริมเข้ามาก็ไม่เพียงพอที่จะปฏิบัติงานที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างเต็มรูปแบบเพื่อให้สอดคล้องกับมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ในระดับสากลได้ อีกทั้งนายทหารที่จบหลักสูตรก็ยังมีความจำเป็นต้องทำงานสารสนเทศอื่น ๆ ตามที่หน่วยกำหนด จึงควรแยกหลักสูตรการศึกษาให้ชัดเจนซึ่งอาจแยกเป็นคนละหลักสูตร หรือหลักสูตรเดียวกันแต่แยกแขนงหลักสูตร โดยมีแขนงวิทยาการคอมพิวเตอร์ ที่เน้น

เกี่ยวกับการทำงานด้านสารสนเทศให้กับกองทัพบก เช่น การวิเคราะห์และออกแบบระบบงานสารสนเทศ การพัฒนาโปรแกรมเพื่อใช้งานสารสนเทศต่าง ๆ ของกองทัพบก และแขนงความมั่นคงปลอดภัยทางไซเบอร์เป็นการเฉพาะเพื่อเน้นด้านการดูแลระบบเครือข่ายการป้องกันและแก้ปัญหาภัยคุกคามทางไซเบอร์ในระดับต่าง ๆ ให้กับกองทัพบก เป็นต้น ซึ่งจะช่วยให้กองทัพบกไม่ขาดแคลนบุคลากรในการดำเนินการในทุกด้านที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยทางไซเบอร์

**3. สื่อการเรียนการสอนที่เหมาะสม**

เป็นที่ทราบกันดีอยู่แล้วว่าการศึกษาอบรมจำเป็นเป็นต้องมีอุปกรณ์เครื่องมือซึ่งเป็นส่วนสำคัญที่จะต้องมีการจัดหา เพื่อเป็นองค์ประกอบในการจัดทำสื่อการเรียนการสอนที่เหมาะสม ซึ่งหลักสูตรการรักษาความปลอดภัยทางไซเบอร์นอกจากอุปกรณ์การสอนโดยทั่วไปแล้วยังต้องใช้เครื่องมืออื่น ๆ ที่เกี่ยวข้องกับการรับมือกับภัยคุกคามทางไซเบอร์ ทั้งการจำลองเหตุการณ์สถานการณ์ต่าง ๆ เพื่อให้ผู้เรียนได้ฝึกปฏิบัติระบบเครือข่ายที่เป็นเครือข่ายจำลองในระบบปิดเพื่อป้องกันภัยคุกคามที่ทดลองใช้ในแต่ละสถานการณ์เผยแพร่ไปสู่ระบบอื่น ผู้เรียนจะต้องรู้จักเครื่องมือต่าง ๆ ทั้งฮาร์ดแวร์ เช่น เซิร์ฟเวอร์ อุปกรณ์คอมพิวเตอร์ อุปกรณ์เทคโนโลยีสารสนเทศประเภทต่าง ๆ ซอฟแวร์ ทั้งซอฟแวร์ระบบและแอปพลิเคชันที่ใช้งานทั่วไป อีกทั้งซอฟแวร์เพื่อใช้ในการศึกษาหาช่องโหว่ซอฟแวร์ประสงค์ร้าย ซอฟแวร์แอนตี้ไวรัส ซอฟแวร์ในการคำนวณรหัสผ่าน เป็นต้น นอกจากนี้ยังรวมถึงอุปกรณ์เครือข่ายต่าง ๆ และอุปกรณ์ที่ผู้รุกรานใช้เพื่อให้ผู้เรียนตระหนักรู้การใช้ภัยคุกคามแบบต่าง ๆ เช่น อุปกรณ์ดักฟัง การทำงานของคีย์ลอกเกอร์ เป็นต้น

**4. การพัฒนาอาจารย์ผู้สอน**

หัวใจของการศึกษาอบรม นอกจากผู้เรียนแล้วก็คือผู้สอนที่ต้องถ่ายทอดความรู้ให้ผู้เรียนเกิดความรู้ความเข้าใจในศาสตร์นั้น ๆ และเนื่องจากหลักสูตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นเรื่องใหม่ของโรงเรียนนายร้อยพระจุลจอมเกล้าที่จะเปิดหลักสูตรฯ การพัฒนาศักยภาพของอาจารย์จึงเป็นสิ่งที่จำเป็นอย่างยิ่ง การเพิ่มพูนความรู้ความสามารถและทักษะในการปฏิบัติงานของอาจารย์ให้ได้ผลดีให้มีประสิทธิผลและประสิทธิภาพ จะช่วยบรรลุเป้าหมายของการพัฒนาหลักสูตรด้วยเช่นกัน จึงควรมีดำเนินการพัฒนาอาจารย์ผู้สอนในรูปแบบต่าง เช่น

- การผลิตอาจารย์ให้มากขึ้น เนื่องจากหลักสูตรการรักษาความปลอดภัยทางไซเบอร์เป็นเรื่องใหม่ อาจต้องใช้อาจารย์ที่ศึกษาในด้านนี้มาโดยเฉพาะ

- การจัดสรรทุนเพื่อศึกษาต่อทั้งในและนอกประเทศ รวมถึงการศึกษาในรูปแบบออนไลน์

- การบริหารจัดการเพื่อให้อาจารย์ที่มีความรู้ความสามารถมีการพัฒนาตนเองอยู่เสมอ และยังทำหน้าที่รับราชการในโรงเรียนนายร้อยพระจุลจอมเกล้าต่อไป และการจัดการให้มีบุคลากรรุ่นใหม่ทดแทนเพื่อการสอนอย่างต่อเนื่อง

- ความร่วมมือกับสถาบันในระดับอุดมศึกษาอื่น ๆ ทั้งในและต่างประเทศเพื่อให้เกิดเครือข่ายความร่วมมือด้านทรัพยากรบุคคล มีการเชิญผู้เชี่ยวชาญแลกเปลี่ยนอาจารย์ และมีการจัดประชุมวิชาการ เพื่อเป็นการสนับสนุนและยกระดับด้านคุณภาพของการผลิตบุคลากรด้านการสอนให้มีประสิทธิภาพต่อไป

**5. ทักษะที่ควรได้รับจากหลักสูตรวิทยาศาสตรบัณฑิต สาขาการรักษาความมั่นคงปลอดภัยทางไซเบอร์**

นักเรียนนายร้อย โรงเรียนนายร้อยพระจุลจอมเกล้าควรมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ด้านต่างๆ ดังนี้

1. ด้านภัยคุกคาม การโจมตีและช่องโหว่

- มีความรู้ความเข้าใจเกี่ยวกับชนิดและประเภทต่าง ๆ ของซอฟแวร์ประสงค์ร้าย (Malware) เช่น ไวรัส (Virus) ซอฟแวร์เรียกค่าไถ่ (Ransomware) หนอนคอมพิวเตอร์ (Worm) โทรจัน (Trojan) เป็นต้น
- เปรียบเทียบและระบุความแตกต่างของการโจมตีประเภทต่าง ๆ เช่น Social engineering, การโจมตีซอฟแวร์และการบริการอื่น ๆ (Application/service attacks) , การโจมตีเครือข่ายไร้สาย (Wireless attacks), การโจมตีการเข้ารหัส (Cryptographic attacks)
- มีความรู้ความเข้าใจประเภทของการบุกรุก เช่น Script Kiddies , Hacktivist , Insiders , Competitions
- มีความรู้เกี่ยวกับช่องโหว่ของระบบได้ และสามารถเข้าใจผลกระทบที่เกิดจากช่องโหว่นั้นได้
- สามารถอธิบายภาพรวมการเจาะระบบให้ผู้บังคับบัญชารับทราบได้

2. ด้านเทคโนโลยีสารสนเทศ

- มีความรู้เกี่ยวกับอุปกรณ์ระบบเครือข่ายที่มีความมั่นคงปลอดภัย เช่น Firewall , VPN concentrator, Router เป็นต้น
- มีความรู้เกี่ยวกับซอฟแวร์สำหรับประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างเหมาะสม
- มีความรู้เกี่ยวกับแก้ไขปัญหาด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศขั้นพื้นฐาน

3. ด้านสถาปัตยกรรมและการออกแบบ

- มีความรู้เกี่ยวกับแนวคิดสถาปัตยกรรมเครือข่ายที่ปลอดภัย และการออกแบบระบบที่ปลอดภัยได้
- สามารถแนะนำการพัฒนาแอปพลิเคชันที่ปลอดภัยได้
- สามารถดำเนินการเพื่อลดความเสี่ยงด้วยระบบอัตโนมัติได้
- ให้ความสำคัญของการรักษาความปลอดภัยทางกายภาพ

4. ด้านการจัดการข้อมูลประจำตัว และการเข้าถึง

- มีความรู้เกี่ยวกับความแตกต่างของการพิสูจน์ตัวตนและการจัดการการเข้าถึงระบบ (Access management)
- มีความรู้เกี่ยวกับระบบพิสูจน์ตัวตนและการเข้าถึงระบบ
- การบริหารจัดการบัญชีผู้ใช้ (Account Management)

5. ด้านการจัดการความเสี่ยง

- กำหนดความสำคัญของนโยบาย แผนการดำเนินงาน ขั้นตอนการปฏิบัติที่ส่งผลกระทบกับความปลอดภัยของหน่วย
- วิเคราะห์ปัจจัยที่มีผลกระทบกับหน่วย
- จัดทำกระบวนการการจัดการความเสี่ยง
- มีความรู้เกี่ยวกับการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น
- การเก็บรวบรวมหลักฐานทางดิจิทัลพื้นฐาน
- จัดทำแผนกู้คืนภัยพิบัติ
- จัดทำนโยบายความเป็นส่วนตัวและการส่งข้อมูลออกไปภายนอก

6. การเข้ารหัส

- มีความรู้การเข้ารหัสขั้นพื้นฐาน
- มีคามรู้เกี่ยวกับความปลอดภัยของระบบเครือข่ายไร้สาย

7. ด้านการตอบโต้เหตุการณ์บนโลกไซเบอร์

- มีความรู้เกี่ยวกับข้อมูลภัยคุกคาม เพื่อกำหนดผลกระทบของเหตุการณ์ และรู้จักชุดเครื่องมือที่เหมาะสม สร้างกลยุทธ์การสื่อสาร พร้อมแนวทางปฏิบัติในการตอบโต้
- สามารถดำเนินการและสรุปแนวทางปฏิบัติที่ดีที่สุดป้องกันผลกระทบต่อหน่วยได้

## ข้อเสนอแนะ

การทำวิจัยครั้งต่อไป ในการทำการวิจัย มีข้อเสนอแนะดังนี้

1.ควรศึกษาปัจจัยด้านความรู้ทางด้านเทคโนโลยีสารสนเทศ ซึ่งอาจส่งผลต่อความตระหนักถึงภัยคุกคามทางไซเบอร์ของกลุ่มตัวอย่าง

2.ควรศึกษาการใช้งานของกลุ่มตัวอย่าง ว่ามีการใช้งานทางไซเบอร์มากน้อยเพียงใด ประเด็นใดบ้าง เพื่อศึกษาความเสี่ยงของภัยคุกคามทางไซเบอร์

3. ควรจะใช้วิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ด้วยการสัมภาษณ์กลุ่ม (Focus Group Interview) หรือการสัมภาษณ์เจาะลึก (In-depth Interview) เพื่อศึกษาความตระหนักภัยคุกคามทางไซเบอร์ของผู้ที่เกี่ยวข้องกับกลุ่มตัวอย่าง เช่น ผู้บังคับบัญชา อาจารย์ เพื่อให้ได้ข้อมูลที่รอบด้านครบทุกมิติมากยิ่งขึ้น

4. ควรมีการศึกษานโยบายของรัฐ กระทรวงกลาโหม กองทัพบก และองค์กรต่าง ๆ ที่เกี่ยวกับการป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในอนาคต

## ข้อจำกัดในการวิจัย

การศึกษาในครั้งนี้มีข้อจำกัดด้านระยะเวลาในการค้นคว้า ซึ่งหากมีเวลาในการค้นคว้ามากขึ้น จะทำให้การศึกษาปัจจัยที่มีผลกระทบต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ในข้อมูลเชิงลึกได้มากขึ้น