การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยง ต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล

ดำรงศักดิ์ สัตบุตร

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาหลักสูตรนิเทศศาสตรมหาบัณฑิต
สาขาวิชานิเทศศาสตร์ คณะนิเทศศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์
พ.ศ. 2564

DEVELOPMENT OF A COMMUNICATION MODEL FOR PREDICTING DIGITAL MEDIA DECEPTION RISKS USING DATA MINING TECHNIQUES

Damrongsak Sattabut

A Thesis Submitted in Partial Fulfillment of the Requirements

For the Degree of Master Communication Arts

Department of Communication Arts

Faculty of Communication Arts, Dhurakij Pundit University

2021

ใบรับรองวิทยานิพนธ์

คณะนิเทศศาสตร์ มหาวิทยาลัยธุรกิจบัณฑิตย์

ปริญญา นิเทศศาสตรมหาบัณฑิต

หัวข้อวิทยานิพนธ์ การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล

เสนอโดย นายดำรงศักดิ์ สัตบุตร

สาขาวิชา นิเทศศาสตร์ กลุ่มวิชาการสื่อสารการตลาดและแบรนด์

อาจารย์ที่ปรึกษาวิทยานิพนธ์ ผู้ช่วยศาสตราจารย์ ดร.กัญญรัตน์ หงส์วรนันท์

ได้พิจารณาเห็นชอบโดยคณะกรรมการสอบวิทยานิพนธ์แล้ว

.....ประธานกรรมการ

(ดร.มนต์ ขอเจริญ)

.....กรรมการและอาจารย์ที่ปรึกษาวิทยานิพนธ์

(ผู้ช่วยศาสตราจารย์ ดร.กัญญรัตน์ หงส์วรนันท์)

..... กรรมการ

(ผู้ช่วยศาสตราจารย์ ดร.กันยารัตน์ ศรีวิสทิยกุล)

คณะนิเทศศาสตร์รับรองแล้ว

.....คณบดีคณะนิเทศศาสตร์

(อาจารย์ กอบกิจ ประดิษฐผลพานิช)

วันที่ ๒๗ เดือน กรกฎาคม พ.ศ. 2564

หัวข้อวิทยานิพนธ์	การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล
ชื่อผู้เขียน	ดำรงศักดิ์ สัตบุตร
อาจารย์ที่ปรึกษา	ผู้ช่วยศาสตราจารย์ ดร.กัญญรัตน์ หงส์วรนันท์
สาขาวิชา	นิเทศศาสตร์ (การสื่อสารการตลาดและแบรนด์)
ปีการศึกษา	2563

บทคัดย่อ

การวิจัยครั้งนี้มีวัตถุประสงค์ (1) เพื่อศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล และ (2) เพื่อพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล ใช้ระเบียบวิธีวิจัยและพัฒนา โดยใช้แบบสอบถามในการเก็บรวบรวมข้อมูล กลุ่มตัวอย่างคือผู้รับสารกลุ่มดิจิทัลเนทีฟไทย อายุระหว่าง 18-36 ปี ทั้งเพศชายและเพศหญิงที่มีประสบการณ์ใช้งานอินเทอร์เน็ตเป็นประจำอย่างน้อย 5 ปี จำนวน 1,067 คน วิเคราะห์ข้อมูลด้วยโปรแกรมสำเร็จรูป ใช้สถิติเชิงพรรณนา ได้แก่ การหาค่าเฉลี่ย การดำเนินการวิจัยแบ่งเป็น 2 ระยะดังนี้ ระยะที่ 1 การศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล และระยะที่ 2 การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล

ผลการวิจัยพบว่า 1) ผลการศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล ได้ปัจจัยจำนวน 9 ปัจจัย ประกอบด้วย อ้างเป็นบุคคลสำคัญ การสร้างความน่าเชื่อถือ กระตุ้นความสนใจ กระตุ้นความต้องการ สร้างความคาดหวัง ความกลัว ความโลภ ความอยากรู้อยากเห็น และการตัดสินใจอย่างไม่มีเหตุผล 2) ผลการพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล พบว่าเทคนิคต้นไม้ตัดสินใจ J48 โดยใช้วิธีการสร้างแบบแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน 80:20 จะมีค่าความถูกต้องสูงที่สุดคิดเป็นร้อยละ 95.49 เมื่อเทียบกับเทคนิคและวิธีการสร้างแบบจำลองแบบอื่น

คำสำคัญ: แบบจำลองด้านการสื่อสาร, ภัยคุกคามทางคอมพิวเตอร์, การทำเหมืองข้อมูล, ฟิชชิ่ง

Thesis Title	Development of a Communication Model for Predicting Digital Media Deception Risks using Data Mining Techniques
Author	Damrongsak Sattabut
Thesis Advisor	Assistant Professor Dr.Kanyarat Hongvoranant
Department	Communication Arts
Academic Year	2020

ABSTRACT

The study aimed to (1) investigate communication factors that influence digital media deception risks, and (2) develop a communication model for predicting digital media deception risks using data mining techniques. The study was carried out using the Research and Development (R&D) methodology, with a questionnaire serving as the data collection instrument. The sample group consisted of 1,067 males and females between the ages of 18 and 36 who were digital native Thai recipients with at least five years of regular internet use. The data was analyzed using a package program that included descriptive statistics for mean investigation. The study was divided into two phrases: (1) studying the communication factors influencing digital media deception risks, and (2) developing a communication model for predicting digital media deception risks using data mining techniques.

The findings revealed that 1) the communication factors influencing digital media deception risks were associated with 9 factors, including key-person impersonation, credibility building, attention gaining, needs stimulation, expectation, fear, greed, as well as curiosity and unreasonable decision making. 2) The effect of communication model development for predicting digital media deception risks using data mining techniques revealed that the Decision Tree techniques (J48), in which the dataset was divided into a training dataset and a testing dataset at 80:20 respectively, achieved an accuracy of 95.49 percent when compared to the other techniques and model development.

Keywords: Communication Model, Computer threats, Data Mining, Phishing

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลุล่วงได้ ด้วยความอนุเคราะห์อย่างดียิ่งจาก ผู้ช่วยศาสตราจารย์ ดร.กัญญรัตน์ หงส์วรนันท์ อาจารย์ที่ปรึกษาวิทยานิพนธ์ ที่ได้ให้คำปรึกษา ชี้แนะ และตรวจสอบแก้ไขข้อบกพร่องต่าง ๆ ในระหว่างการทำวิจัย จึงทำให้วิทยานิพนธ์ฉบับนี้เสร็จสมบูรณ์ และขอกราบขอบพระคุณ ดร.มนต์ ขอเจริญ และ ผู้ช่วยศาสตราจารย์ ดร.กันยารัตน์ ศรีวิสทิยกุล ที่ได้ให้ความกรุณารับเป็นกรรมการในการสอบวิทยานิพนธ์ และได้ให้ข้อเสนอแนะเพิ่มเติมสำหรับการทำวิทยานิพนธ์ให้มีความสมบูรณ์ยิ่งขึ้น ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูงไว้ ณ ที่นี้

ขอขอบคุณ ว่าที่ร้อยตรี ชัยชนะ กุลวรฐิต ที่ให้คำแนะนำและช่วยเหลือด้านเทคนิคมาโดยตลอด และขอขอบคุณผู้ตอบแบบสอบถามทุกท่าน ที่กรุณาสละเวลาให้ข้อมูลจนผู้วิจัยสามารถนำมาพัฒนาเป็นแบบจำลองได้

สุดท้ายนี้ คุณงานความดีอันใดที่เกิดจากการทำวิทยานิพนธ์ฉบับนี้ ข้าพเจ้าขอมอบให้กับบิดามารดา ตลอดจนคณาจารย์ที่เคารพ ที่ได้ประสิทธิ์ประสาทวิชาความรู้และถ่ายทอดประสบการณ์ที่ดีให้แก่ข้าพเจ้า

ดำรงศักดิ์ สัตบุตร

สารบัญ

หน้า

สารบัญ (ต่อ)

บทที่ **หน้า**

สารบัญตาราง

ตารางที่ **หน้า**

สารบัญรูปภาพ

ภาพที่ **หน้า**

สารบัญรูปภาพ (ต่อ)

ภาพที่ **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

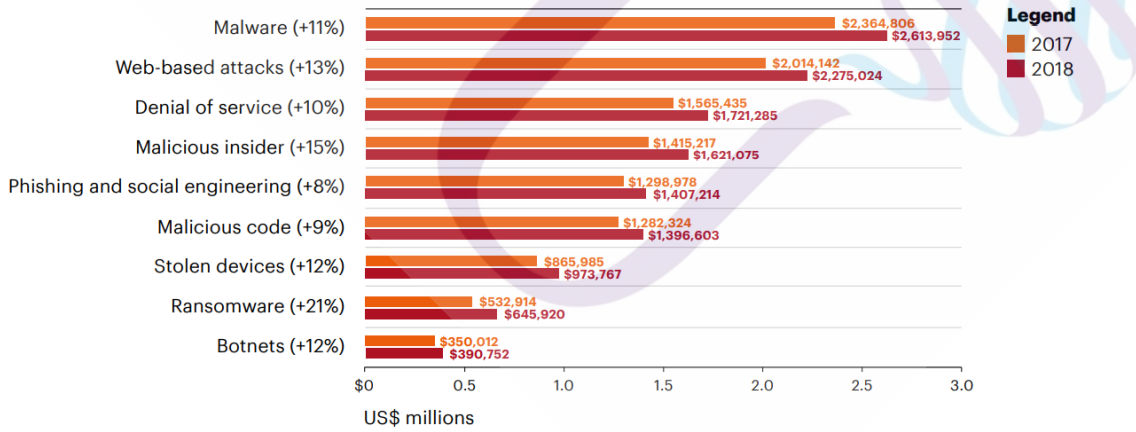
จากรายงานการใช้ดิจิทัล ประจำเดือนกรกฎาคม 2563 จัดทำโดย We Are Social ดิจิทัล เอเจนซี่ และ Hootsuite ผู้ให้บริการระบบจัดการ Social Media และ Marketing ระดับโลก (Simon Kemp, 2020) พบภาพรวมพฤติกรรมการใช้งานสื่อดิจิทัลของคนทั่วทั้งโลกดังนี้ มีประชากรทั่วโลกมีอยู่ราว 7.79 พันล้านคน ใช้งานโทรศัพท์มือถือจำนวน 5.15 พันล้านคน ใช้งานสื่อโซเชียล 3.96 พันล้านคน โดยในจำนวนประชากรทั้งหมดนี้เป็นผู้ใช้งานอินเทอร์เน็ตสูงถึง 4.57 พันล้านคน หรือคิดเป็นร้อยละ 58.69 ของประชากรทั้งหมด

เทคโนโลยีอินเทอร์เน็ต นับได้ว่าเป็นจิ๊กซอว์ตัวสำคัญทางดิจิทัลที่ได้เข้ามาเติมเต็มสรรสร้างสังคมทุกมิติ ตั้งแต่การใช้ชีวิตประจำวัน การศึกษา การดำเนินธุรกิจ รวมถึงเป็นกลไกสำคัญในการขับเคลื่อนเศรษฐกิจทั้งในระดับจุลภาคและมหภาค การเชื่อมต่อ ติดต่อสื่อสารไปยังอีกซีกโลกหนึ่งเป็นสามารถทำได้ในเวลาเพียงเสี้ยววินาที แต่ทว่ายิ่งสะดวกรวดเร็วมากขึ้นเท่าใด อินเทอร์เน็ตก็ยังสามารถส่งผลเสีย และกระจายภัยคุกคามได้รวดเร็วมากยิ่งขึ้นเท่านั้น โดยเฉพาะอย่างยิ่งเมื่อผู้คน สามารถเชื่อมต่อกับอินเทอร์เน็ตได้ ก็ยิ่งเป็นการเปิดโอกาสให้เหล่าผู้ไม่หวังดีพัฒนา ไวรัส มัลแวร์ รวมไปถึงกลวิธีใหม่ ๆ ที่สามารถสร้างผลกระทบให้กับผู้ใช้งาน เมื่อผู้ใช้งานไม่ตระหนักถึงภัยคุกคาม ขาดการรู้เท่าทัน และประมาทเลินเล่อต่อคำเตือนบนหน้าจอ ก็เป็นอีกสาเหตุที่ทำให้ภัยคุกคามต่าง ๆ นั้นเกิดได้ง่ายขึ้น

อาชญากรรมทางไซเบอร์ (Cybercrime) หมายถึง กิจกรรมที่ผิดกฎหมายใด ๆ ที่ใช้หรือรุกรานระบบและเครือข่ายคอมพิวเตอร์ รวมไปถึงอินเทอร์เน็ต (Capgemini 2012, อ้างถึงใน Thaire Group, 2015) ซึ่งสามารถแบ่งการโจมตีออกเป็นใน 3 รูปแบบดังนี้ 1) การทำให้ธุรกิจหยุดชะงักหรือล่วงละเมิด (Business disruption and misuse) เช่น ทำให้ระบบคอมพิวเตอร์หยุดทำงานหรือ

ทำงานได้อย่างไม่มีประสิทธิภาพ 2. การหลอกลวงทางออนไลน์ (Online scam) เช่น การหลอกขายสินค้าและหลอกโอนเงินบนโลกออนไลน์ และ 3. การลักขโมยและฉ้อโกงเพื่อผลประโยชน์ (Theft and fraud) เช่น การขโมยอัตลักษณ์ของเหยื่อไปทำธุรกรรมทางการเงิน

นิตยสารด้านความปลอดภัยทางคอมพิวเตอร์ ประเทศสหรัฐอเมริกาทำนายว่าในปี 2564 อาชญากรรมไซเบอร์ (Cybercrime) จะก่อให้เกิดความเสียหายทั่วโลกรวมกันสูงถึง 6 ล้านล้านดอลลาร์สหรัฐ ซึ่งเพิ่มขึ้น 3 ล้านล้านดอลลาร์จากปี 2558 สะท้อนให้เห็นการถ่ายโอนความมั่งคั่งทางเศรษฐกิจในตลาดมืด ซึ่งเป็นแรงจูงใจดึงดูดผู้ไม่หวังดีให้ก่ออาชญากรรมทางไซเบอร์ เพราะเป็นการลงทุนที่น้อยกว่า แต่สามารถทำกำไรได้มากกว่าการค้ายาเสพติดทั่วโลกรวมกัน (Cybersecurity Ventures, 2020) สอดคล้องกับรายงาน The cost of cyber crime ที่สัมภาษณ์ 2,647 หัวหน้างาน จาก 355 บริษัท 16 ประเภทธุรกิจ ใน 11 ประเทศ พบว่า การขยายตัวของนวัตกรรมและธุรกิจใหม่ ๆ นำไปสู่การเพิ่มขึ้นของการโจมตีทางอินเทอร์เน็ต โดยเฉลี่ยแล้วในปีที่ผ่านมาขึ้นเพิ่ม 11 เปอร์เซ็นต์ ทำให้องค์กรต่างๆ ต้องแบกรับต้นทุนด้านการจัดการความปลอดภัยเพิ่มขึ้น สาเหตุที่องค์กรต้องให้ความสำคัญกับประเด็นนี้เป็นเพราะอาจส่งผลต่อความน่าเชื่อถือจากลูกค้าและนักลงทุน โดยประเทศที่ตกเป็นเหยื่อจากอาชญากรรมไซเบอร์ 5 อันดับแรก คือ สหรัฐอเมริกา, ญี่ปุ่น, เยอรมนี, สหราชอาณาจักร และฝรั่งเศส



ภาพที่ 1.1 ประเภทของการโจมตีทางไซเบอร์และต้นทุนรักษาความปลอดภัยที่บริษัทต้องแบกรับในปี 2017 และ 2018

ที่มา: Accenture, 2019

ซึ่งภัยไซเบอร์มุ่งโจมตีทั้งตัวบุคคล ภาครัฐ และภาคเอกชน โดยในปี 2018 ต้นทุนรักษาความปลอดภัยไซเบอร์ในการโจมตีประเภทต่างๆ มีแนวโน้มพุ่งสูงขึ้นอย่างเห็นได้ชัด เป็นผลมาจากการพัฒนารุดหน้าของเทคโนโลยี โดย 5 อันดับภัยไซเบอร์ที่บริษัทจะต้องเสียค่าใช้จ่ายในการดูแลป้องกันคือ Malware, Web-based attacks, Denial of service, Malicious insider และ Phishing and social engineering (Accenture, 2019)

โดยไทยเซิร์ต (2563) พบว่า คนไทยเสี่ยงต่อถูกการโจมตีประเภท Malicious Code การติดตั้งโปรแกรมที่มีคำสั่งที่สร้างความเสียหายต่อเครื่องผู้ใช้ เช่น การสอดแนมหรือขโมยข้อมูลของผู้ใช้งาน มากที่สุด ตามด้วย Fraud การใช้ข้อมูลโดยไม่ได้รับอนุญาต การละเมิดลิขสิทธิ์ รวมไปถึงการโจมตีที่ปลอมตัวเป็นนิติบุคคลหนึ่งที่ได้รับประโยชน์จากการปลอมตัวเป็นนิติบุคคลอื่น (WP4 Clearinghouse Policy, 2003) การปลอมแปลงเป็นบุคคลอื่นเพื่อหลอกเอาข้อมูลจากผู้ใช้งานนั้นมีมาตั้งแต่ปี 2538 (cofense) โดยนิยมใช้วิธีที่เรียกว่า ฟิชชิ่ง (Phishing) ซึ่งมักจะปลอมแปลงเป็นบุคคล หน่วยงาน หรือแหล่งข้อมูลที่น่าเชื่อถือส่ง URL ให้เหยื่อคลิก เข้าถึง และกรอกข้อมูล โดยการทำฟิชชิ่งยังสามารถโจมตีผ่านทางช่องทางอื่น ๆ ได้อีก อาทิ สื่อสังคมออนไลน์ เฟซบุ๊ก ทวิตเตอร์ เว็บไซต์ ต่างๆ เป็นต้น (Institute of Information Security, 2014 อ้างถึงใน พงศ์พนธ์ ภาวศุทธิ์, 2561)

อันตรายของการโจมตีประเภทฟิชชิ่ง คือการนำข้อมูลที่หลอกได้จากผู้ใช้ ไม่ว่าจะด้วยวิธีการใดก็ตามแต่ ไปใช้ประโยชน์ต่อในทางที่ไม่ถูกต้อง ดังเช่นกรณีที่ “ทวิตเตอร์” ถูกผู้ไม่หวังดีปลอมแปลงเป็นเว็บไซต์ภายใน ทำให้พนักงานระดับสูงหลงเชื่อและให้ข้อมูลการเข้าสู่ระบบกับเว็บไซต์ปลอมดังกล่าว

ภาพที่ 1.2 บัญชีผู้ใช้งานทวิตเตอร์ของ บิล เกตส์ ถูกผู้ไม่หวังดีโพสต์ข้อความหลอกลวง

ที่มา: Bobby Allyn, 2019

ส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงบัญชีผู้ใช้ที่มีชื่อเสียงในสังคม เช่น อดีตประธานาธิบดีสหรัฐ บารัค โอบาม่า, ผู้บริหารบริษัท เทสล่า อีลอน มัสก์, ผู้ก่อตั้งบริษัทไมโครซอฟท์ บิล เกตส์ เป็นต้น โพสต์หลอกลวงให้ประชาชนหลงเชื่อและโอนเงิน จากเหตุการณ์ดังกล่าวทำให้มีผู้ตกเป็นเหยื่อจำนวนมากซึ่งมีมูลค่าความเสียหายในครั้งนี้สูงถึง 1 แสนดอลลาร์สหรัฐ (Twitter Inc., 2020)

ในขณะที่ประเทศไทยก็พบกับเหตุการณ์การโจมตีด้วยฟิชชิ่ง ดังเช่น กรณีปลอมแปลงเป็นบริษัทโทรคมนาคมโทรศัพท์ติดต่อไปยังเหยื่อเพื่อหลอกขอรหัสผ่านแบบครั้งเดียว (One Time password) เข้าสู่ระบบธนาคารออนไลน์ ท้ายที่สุดผู้ไม่หวังดีสามารถโอนเงินออกจากบัญชีของเหยื่อไปได้สูงถึง 400,000 บาท (Workpoint, 2563) นอกจากนี้ยังพบรูปแบบการล่อลวงโดยการปลอมแปลงเว็บไซต์แจกแบบสอบถาม อ้างหากตอบแบบสอบถามครบจะได้รับโทรศัพท์รุ่นดังฟรี ซึ่งทางบริษัทได้ออกมาปฏิเสธในภายหลังว่าไม่ได้เป็นผู้จัดกิจกรรมดังกล่าว และขอให้ระวังการกรอกข้อมูลส่วนบุคคล

ภาพที่ 1.3 การปลอมแปลงเป็นเว็บไซต์ เพื่อหลอกขอข้อมูลจากเหยื่อ

ที่มา: Yokekung (2563)

นอกจากนี้ยังพบว่าผู้รับสารที่เป็นกลุ่มดิจิทัลเนทีฟ (Digital Natives) (Herther, 2009 อ้างถึงใน สสินาท แสงทองฉาย, 2560) ซึ่งเป็นกลุ่มที่คุ้นชินกับการใช้สื่อดิจิทัล มีทักษะการใช้อุปกรณ์อิเล็กทรอนิกส์ และเทคโนโลยีในระดับที่สูง มีอุปกรณ์การสื่อสารที่สามารถเข้าถึงอินเทอร์เน็ตได้ มีแนวโน้มที่จะโดนโจมตีด้วยวิธีฟิชชิ่งสูงกว่าผู้คนในกลุ่มอื่น จากรายงานพยากรณ์ภัยคุกคามและความมั่นคงปลอดภัยของ Forcepoint (2007) ระบุว่า กลุ่มคนที่เติบโตมาพร้อมกับอินเทอร์เน็ตและเทคโนโลยี จะมีการเปิดใจและเชื่อมั่นในการใช้เทคโนโลยีต่าง ๆ ส่งผลให้สามารถประยุกต์ใช้ในการทำงานได้อย่างมีประสิทธิภาพสูงสุด แต่การที่ใกล้ชิดและใช้งานเทคโนโลยีต่าง ๆ มากเกินไป ทำให้ขาดความตระหนักถึงความมั่นคงปลอดภัยและความเป็นส่วนบุคคล ก่อให้เกิดช่องโหว่ที่แฮ็กเกอร์สามารถนำไปใช้ ซึ่งสอดคล้องกับผลลัพธ์ของ Vasileios Gkioulos (2017) ที่ศึกษาเรื่องการรับรู้ความปลอดภัยของกลุ่มดิจิทัลเนทีฟ พบว่าคนกลุ่มดิจิทัลเนทีฟมีความมั่นใจในการใช้งานอุปกรณ์เคลื่อนที่ อาทิ สมาร์ทโฟน แท็บเล็ต แล็ปท็อป ในชีวิตประจำวัน ซึ่งนำไปสู่พฤติกรรมที่เพิกเฉยต่อการกระทำที่อาจจะเกิดผลกระทบต่อความปลอดภัย แต่อย่างไรก็ตามเมื่อคนกลุ่มดิจิทัลเนทีฟรับรู้ถึงภัยคุกคามทางไซเบอร์ กลุ่มคนเหล่านี้จะสามารถปรับเปลี่ยนพฤติกรรม และรักษาความปลอดภัยของตนได้ดีมากยิ่งขึ้น

ทั้งนี้มีปัจจัยหลากหลายรูปแบบที่ส่งผลให้การโจมตีด้วยวิธีฟิชชิ่งสำเร็จผล อาทิ ปัจจัยส่วนบุคคล รวมไปถึงปัจจัยทางด้านการสื่อสาร ผู้ส่งสาร (Sender) เนื้อหาสาร (Messages) ช่องทาง (Channel) และ ผู้รับสาร (Receiver) ที่แฮ็กเกอร์ใช้เพื่อสร้างความน่าเชื่อถือ สร้างความตื่นตระหนก และก่อให้เกิดพฤติกรรมอันตรายทางไซเบอร์ของผู้ตกเป็นเหยื่อ

ในด้านผู้ส่งสาร (Sender) แฮ็กเกอร์จะใช้ประโยชน์จากการแอบอ้างเป็นหน่วยงานของภาครัฐ บุคคลหรือองค์กรที่น่าเชื่อถือ ดังเช่นกรณีแก๊งต้มตุ๋น อ้างเป็นเจ้าหน้าที่ธนาคารให้บริการปล่อยสินเชื่อเงินกู้ โดยหลอกขอข้อมูลส่วนตัว อาทิ ชื่อ-สกุล รหัสประจำตัวประชาชน รหัสล็อกอินเข้าสู่ระบบธนาคารออนไลน์ เมื่อเหยื่อหลงเชื่อและมอบข้อมูลให้ คนร้ายจะนำข้อมูลดังกล่าวไปเข้าสู่ระบบธนาคารและโอนเงินออกจากบัญชี ในกรณีนี้มีผู้เสียหายทั้งสิ้นกว่า 20 ราย เป็นมูลค่าความเสียหายรวมกว่า 2 ล้านบาท (ไทยรัฐออนไลน์, 2564จ) ในต่างประเทศไอบีเอ็มพบแฮ็กเกอร์ปลอมแปลงอีเมลสูงขึ้นกว่า 6,000% โดยอ้างตัวเป็นหน่วยงานด้านสาธารณสุข และหน่วยงานที่จะ

ช่วยเหลือเยียวยาประชาชนจากสถานการณ์การแพร่ระบาดของโรคโควิด-19 (ไทยรัฐออนไลน์, 2563ข)

ด้านเนื้อหาสาร (Message) แฮ็กเกอร์จะใช้ถ้อยคำหรือข้อความกระตุ้นความสนใจหรือความต้องการ รวมไปถึงสร้างความคาดหวัง เพื่อให้เหยื่อหลงเชื่อ ดังเช่นกรณีเหยื่อได้รับข้อความทาง SMS แจ้งให้อัปเดตข้อมูลกับธนาคารทันทีพร้อมแนบลิงก์ปลอม ซึ่งคนร้ายจะนำข้อมูลดังกล่าวที่ได้ไปถอนเงินผ่านตู้ ATM หรือแอปพลิคชัน ในกรณีนี้มีผู้เสียหายทั้งสิ้นกว่า 19 ราย คิดเป็นมูลค่าความเสียหายรวมกว่า 1.9 ล้านบาท (พีพีทีวีออนไลน์, 2563ก)

ด้านช่องทาง (Channel) แฮ็กเกอร์จะอาศัยธรรมชาติของสื่อในการหลอกขอข้อมูลของเหยื่อ โดยวิธีการฟิชชิ่งแฮ็กเกอร์สามารถใช้ตั้งแต่ โทรศัพท์ (Vishing) ข้อความสั้น (Smishing) ไปจนถึงสื่อสังคมออนไลน์ ดังเช่นกรณียายชาวฮ่องกง โดนแก๊งต้มตุ๋น ปลอมเป็นเจ้าหน้าที่ตำรวจจากประเทศจีนโทรศัพท์มาหาเธอโดยอ้างว่าข้อมูลส่วนตัวของเธอถูกนำไปใช้ในการก่ออาชญากรรม โดยเหยื่อคนดังกล่าวหลงเชื่อและโอนเงินเป็นค่าดำเนินการสูงถึง 1,000 ล้านบาท (ไทยรัฐออนไลน์, 2564ง)

และด้านผู้รับสาร (Receiver) แฮ็กเกอร์จะใช้ประเด็นด้านความกลัว ความโลภ ความอยากรู้อยากเห็น รวมไปถึงการตัดสินใจอย่างไม่มีเหตุผลของเหยื่อ ดังเช่นกรณี หญิงวัย 62 ปี ถูกคนร้ายแอบอ้างเป็นทนายประสานงานจับคนร้ายแก๊งคอลเซ็นเตอร์ที่ตนถูกหลอกไปก่อนหน้า โดยอ้างว่าถ้าฟ้องชนะจะได้เงินหลักล้าน ทำให้เหยื่อหลงเชื่อโอนเงินรวมกว่า 4 แสนบาท (พีพีทีวีออนไลน์, 2563ข)

จากปัญหาดังกล่าวจะเห็นได้ว่าวิธีการล่อลวงบนสื่อดิจิทัลเป็นอาชญากรรมทางไซเบอร์ที่ร้ายแรงระดับโลก ซึ่งรวมถึงประเทศไทยที่กำลังประสบปัญหาเสียหายกับระบบเศรษฐกิจที่มีแนวโน้มจำนวนมากขึ้นอย่างต่อเนื่อง ซึ่งการใช้ซอฟต์แวร์ในการป้องกันเพียงอย่างเดียวยังไม่สามารถตอบโจทย์ได้ เพราะกลวิธีต่าง ๆ ที่ผู้ไม่หวังดีมักจะมุ่งเน้นการโจมตีไปที่ปัจเจกบุคคล โดยอาศัยลักษณะทางสารสนเทศ ทั้งข้อความ ช่องทาง ความน่าเชื่อถือของผู้ส่ง รวมถึงปัจจัยส่วนบุคคลของเหยื่อ มาเป็นองค์ประกอบสำคัญในการก่ออาชญากรรมในแต่ละครั้ง ซึ่งผู้วิจัยมีความสนใจที่จะศึกษาปัญหาที่เกิดขึ้น เพื่อค้นหาปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวง และนำเทคนิคเหมืองข้อมูลมาใช้ในการวิเคราะห์ความสัมพันธ์เพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล

1.2 วัตถุประสงค์การวิจัย

1. เพื่อศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

2. เพื่อพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล

1.3 สมมติฐาน

1. ปัจจัยด้านการสื่อสารมีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

2. ปัจจัยด้านการสื่อสารและปัจจัยส่วนบุคคลมีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

3. แบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล มีค่าความถูกต้อง (Accuracy) อยู่ในระดับสูง

1.4 ประโยชน์ที่คาดว่าจะได้รับ

1. ประโยชน์ในเชิงวิชาการ การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล เป็นการประยุกต์ใช้ทฤษฎีทางด้านนิเทศศาสตร์และเทคโนโลยีสารสนเทศมาค้นหาปัจจัยการสื่อสารที่มีส่วนเกี่ยวข้องอย่างเป็นระบบ มีความถูกต้องแม่นยำ สามารถนำไปประยุกต์ใช้ในการสร้างสื่อประชาสัมพันธ์ สื่อสารความปลอดภัยทางไซเบอร์ ได้ตรงจุดมากยิ่งขึ้น รวมทั้งกระตุ้นให้เกิดการศึกษาวิจัยด้านภัยไซเบอร์อย่างต่อเนื่องให้สอดคล้องกับบริบทสังคมที่มีความเป็นพลวัตต่อไป

2. ประโยชน์ในทางวิชาชีพ เนื่องจากการพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล จะช่วยให้องค์กรภาครัฐ ภาคเอกชน ตลอดจนผู้มีส่วนเกี่ยวข้องเกิดความเข้าใจอย่างลึกซึ้งในองค์ประกอบด้านการสื่อสารที่ทำให้คนไทยถูกล่อลวง และจะได้เตรียมรับมือผ่านการสื่อสาร สร้างสาร ได้ตรงจุด ลดการถูกล่อลวงผ่านโลกดิจิทัลได้มากยิ่งขึ้น

1.5 ขอบเขตของการวิจัย

ขอบเขตของการวิจัยเรื่อง “การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล” ทำการศึกษาโดยแบ่งเป็น 2 ระยะ ดังนี้

ระยะที่ 1 การศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

การศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล เริ่มต้นจากการสังเคราะห์ข้อมูลจากเอกสาร (Documentary Research) เพื่อหาปัจจัย โดยรวบรวมปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล ต่อมานำปัจจัยที่ได้มาตั้งเป็นข้อคำถาม โดยเป็นมาตรวัดของลิเคอร์ท (Likert scale) ประกอบด้วย เห็นด้วยที่สุด เห็นด้วย ไม่แน่ใจไม่เห็นด้วย ไม่เห็นด้วยที่สุด (Safrudiannur, 2020) ตรวจสอบแบบสอบถามโดยผู้ทรงคุณวุฒิจำนวน 3 ท่าน

ระยะที่ 2 การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล

การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล เป็นการศึกษาจากระยะที่ 1 การศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล โดยดำเนินการเก็บข้อมูลจริงกับกลุ่มตัวอย่างซึ่งเป็นผู้รับสารกลุ่มดิจิทัลเนทีฟไทย ที่มีอายุระหว่าง 18 – 36 ปี จำนวน 1,067 คน เนื่องจากมีพฤติกรรม ไลฟ์สไตล์ และการเข้าถึงอินเทอร์เน็ตที่สูงกว่าเจเนอเรชันอื่น หลังจากนั้นจะนำข้อมูลที่ได้ทั้งหมดเข้าสู่กระบวนการของเทคนิคเหมืองข้อมูล (Data Mining Techniques) โดยใช้ซอฟต์แวร์เวกา (WEKA : Waikato Environment for Knowledge Analysis) (Velayutham, 2017) ทำการเปรียบเทียบเทคนิคจำแนกข้อมูลและวิธีการสร้างแบบจำลองที่ให้ค่าความถูกต้อง (Accuracy) สูงที่สุด โดยคัดเลือกวิธีต้นไม้ตัดสินใจ (Decision tree) นาอีฟเบย์ (Naive Baye) และซัพพอร์ตเวกเตอร์แมชชีน (Support Vector Machine) และสรุปแบบจำลองของปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

1.6 นิยามศัพท์

การถูกล่อลวงบนสื่อดิจิทัล หมายถึง การหลงเชื่อและให้ข้อมูลแก่ผู้ไม่หวังดี โดยผู้ไม่หวังดีจะลอกเลียนแบบเป็นองค์กรหรือแหล่งข้อมูลที่น่าเชื่อถือ ผ่านการใช้อีเมลปลอม เว็บไซต์

ปลอม เพื่อให้เหยื่อหลงเชื่อและกระทำการบางอย่าง เช่น การเปิดเผยข้อมูล ชื่อผู้ใช้ รหัสผ่าน รหัสบัตรเครดิตเป็นต้น

ปัจจัยการสื่อสาร (Communication Factors) หมายถึง องค์ประกอบต่าง ๆ ของการสื่อสาร ประกอบด้วย รูปแบบ (Format) เนื้อหา (Content) ช่องทางการสื่อสาร (Channel) และความน่าเชื่อถือของผู้ส่งสาร (Sender) เพื่อให้เกิดความเข้าใจร่วมกันระหว่างผู้ส่งสารและผู้รับสาร

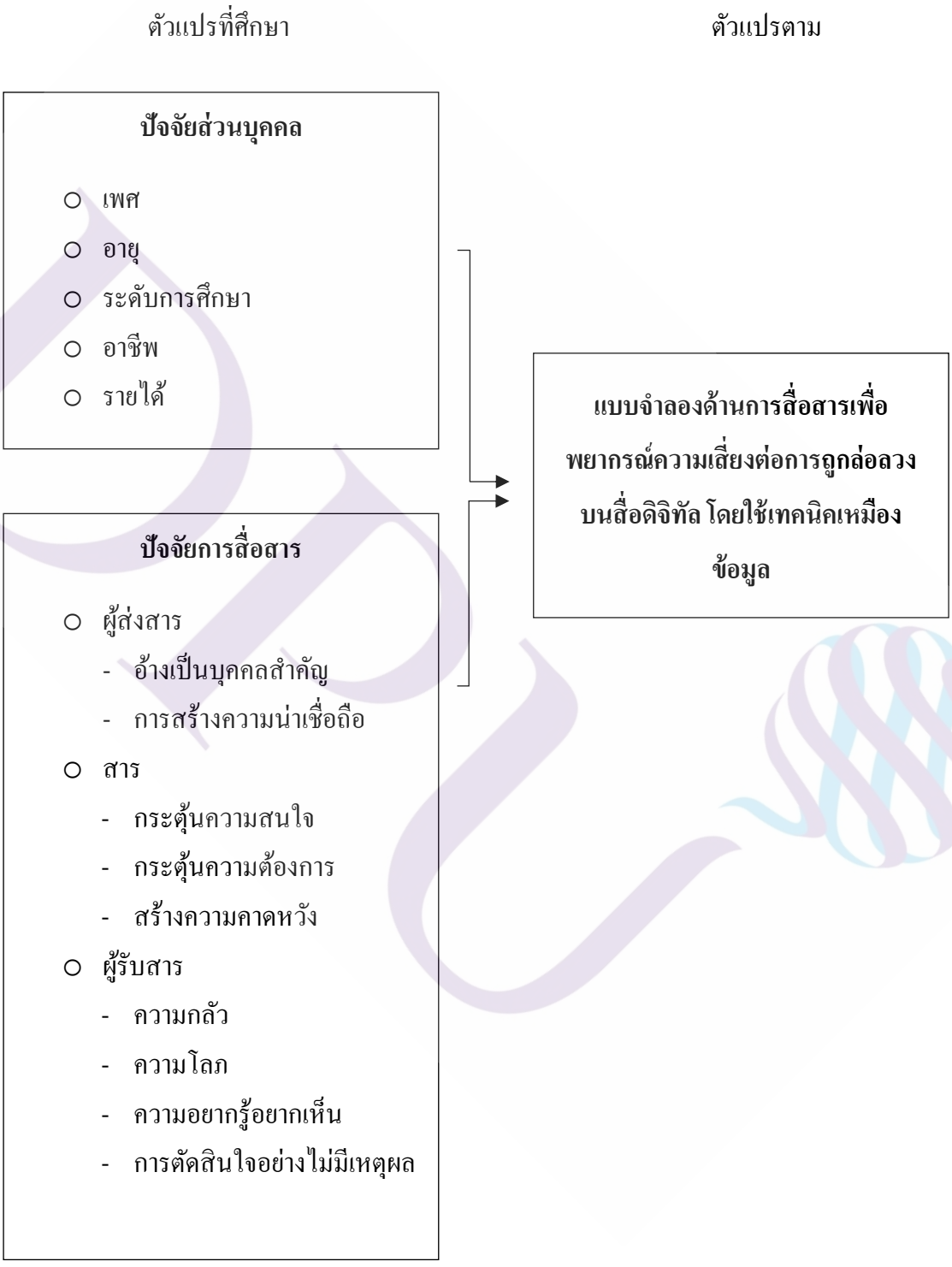
ผู้รับสาร (Receiver) หมายถึง ผู้รับสารในกลุ่มดิจิทัลเนทีฟไทย อายุระหว่าง 18 - 36 ปี มีการใช้งานสื่อสังคมออนไลน์ หรืออินเทอร์เน็ตเป็นประจำทุกวัน ผ่านอุปกรณ์สื่อสารที่สามารถเชื่อมโยงกับเครือข่ายอินเทอร์เน็ตได้

เทคนิคเหมืองข้อมูล (Data Mining Techniques) หมายถึง กระบวนการที่กระทำกับปัจจัยที่ส่งผลต่อการถูกล่อลวงของผู้รับสาร เพื่อค้นหารูปแบบและความสัมพันธ์ที่ซ่อนอยู่ในชุดข้อมูลนั้น ประกอบด้วย 7 ขั้นตอน ได้แก่ 1) การกรอกข้อมูล (Data Cleaning) 2) การรวมข้อมูล (Data Integration) 3) การคัดเลือกข้อมูล (Data Selection) 4) การแปลงรูปแบบข้อมูล (Data Transformation) 5) การค้นหาแบบจำลอง (Pattern Evaluation) และ 6) การนำเสนอความรู้ที่ค้นพบ (Knowledge Representation)

แบบจำลองด้านการสื่อสาร (Communication Model) หมายถึง รูปแบบการเชื่อมโยงที่เชื่อมต่อระหว่างปัจจัยการสื่อสาร เพื่ออธิบายความสัมพันธ์หรือชี้ให้เห็นถึงความเชื่อมโยงหรือลักษณะบางอย่าง

การพยากรณ์ (Predict) หมายถึง การคาดการณ์เหตุการณ์ในอนาคต โดยอาศัยข้อมูลในอดีตที่ถูกทดสอบและพัฒนาเป็นแบบจำลองเรียบร้อยแล้ว

1.7 กรอบแนวคิดในการวิจัย



บทที่ 2
แนวคิด ทฤษฎี และผลงานวิจัยที่เกี่ยวข้อง

ในงานวิจัยเรื่อง “การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล” ผู้วิจัยได้รวบรวมกรอบแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง ดังนี้

2.1 ทฤษฎีการสื่อสารยุคดิจิทัล

2.2 ทฤษฎีและแนวคิดเกี่ยวกับดิจิทัลเนทีฟ

2.3 การถูกล่อลวงบนสื่อดิจิทัล

2.4 เทคนิคเหมืองข้อมูล

2.5 ต้นไม้ตัดสินใจ

2.6 นาอีฟเบย์

2.7 ซัพพอร์ตเวกเตอร์แมชชีน

2.8 งานวิจัยที่เกี่ยวข้อง

2.1 ทฤษฎีการสื่อสารยุคดิจิทัล

2.1.1 ความหมายการสื่อสารยุคดิจิทัล

มีผู้ให้คำจำกัดความของการสื่อสาร (Communication) ไว้หลายคำจำกัดความดังนี้

คาร์ล ไอ โฮฟแลนด์ เออร์วิง แอล เจนิส และ แฮรอลด์ เอช เคลลี (Carl l. Hovland, Irvin L. Janis, & Harold H. Kelly, 1953) อธิบายว่า เป็นกระบวนการที่บุคคลฝ่ายหนึ่งพยายามส่งต่อสิ่งเร้า โดยมีจุดมุ่งหวังเพื่อเปลี่ยนพฤติกรรมของอีกฝ่ายหนึ่ง

คอลิน เชอร์ลี (Colin Cherry, 1957) อธิบายว่า เป็นการกระทำโดยยึดสิ่งเร้าเป็นเครื่องหมายแรก อันจะก่อให้เกิดปฏิกิริยาตอบสนองซึ่งนับได้ว่าเป็นเครื่องหมายอันที่สอง ทั้งนี้ขึ้นอยู่กับผู้รับสารแต่ละคนว่าจะแสดงปฏิกิริยาต่อสิ่งเร้าเหล่านั้นอย่างไร ซึ่งเป็นผลมาจากลักษณะนิสัยและประสบการณ์ในอดีต

แอริสโตเติล (อ้างถึงใน Berlo, 1960) อธิบายว่า เป็นการค้นคว้า วิธีการจูงใจที่มีอยู่ในทุกรูปแบบ

วิลเบอร์ แชรมม์ (Wilbur Schramm, 1974 อ้างถึงใน จินตนา เหมรา, 2558) ให้คำนิยามเกี่ยวกับการสื่อสารว่า เป็นความเข้าใจร่วมในสัญลักษณ์หรือข้อมูลที่แสดงถึงเนื้อหาข่าวสารต่าง ๆ

ชาร์ลส์ อี ออสกูด (Charles E. Osgood, 1974 อ้างถึงใน จินตนา เหมรา, 2558) กล่าวว่า

การสื่อสารจะเกิดขึ้นก็ต่อเมื่อมีฝ่ายหนึ่งเป็นผู้ส่งสาร ซึ่งมีอิทธิพลเหนือกว่าอีกฝ่ายหนึ่งคือผู้รับสาร โดยมุ่งใช้สัญลักษณ์ต่าง ๆ โดยการส่งผ่านสื่อที่ทำหน้าที่เชื่อมต่อระหว่างสองฝ่าย

ปาริชาติ สถาปิตานนท์ (2551) ให้คำนิยามว่า กิจการการในลักษณะต่าง ๆ ที่แตกต่างกันไป โดยเกี่ยวข้องกับบุคคลที่รับบทบาทเป็นแหล่งสาร (Source) ที่ทำหน้าที่นำเสนอหรือแลกเปลี่ยนเรื่องราวและส่งข้อมูลข่าวสารเหล่านั้นผ่านช่องทางการสื่อสาร (Channel) โดยหมายรวมถึงกิจกรรมการสื่อสารระดับบุคคล และกลุ่มบุคคล เช่น การพูดจาหว่านล้อม (Lobbying) การประชุม (Meeting) ไปจนถึงการสื่อสารผ่านสื่อมวลชนแขนงต่าง ๆ (Mass media) หรือการสื่อสารผ่านเทคโนโลยีสมัยใหม่ (New media) ไปสู่ผู้รับสาร

จึงอาจกล่าวได้ว่า การสื่อสาร คือ กระบวนการสื่อความหมาย โดยมีองค์ประกอบทั้งผู้ส่งสาร เนื้อหาสาร ช่องทางการสื่อสาร รวมไปถึงผู้รับสาร โดยมีวัตถุประสงค์ที่ชัดเจนภายใต้บริบทที่แตกต่างกัน

ในขณะที่ วรวุฒิ อ่อนน่วม (2559) ซึ่งศึกษาปรากฏการณ์ทางการสื่อสารยุคดิจิทัล (The Communication Phenomenon in Digital Age) ได้ให้คำนิยามของการสื่อสารยุคดิจิทัลว่า การสื่อสารที่เทคโนโลยีเข้ามามีบทบาทสำคัญ ซึ่งทำให้ผู้รับสารเปลี่ยนแปลงบทบาทตนจากการเป็นผู้รับสารแบบผู้ตาม (Passive Receiver) เป็นผู้รับสารแบบผู้เลือก (Active Audience) ซึ่งสอดคล้องกับ สุรสิทธิ์ วิทยา (2549, อ้างถึงใน วรวุฒิ อ่อนน่วม, 2559) ที่ศึกษาเรื่อง การพัฒนาการสื่อใหม่ พบว่าเป็นการสื่อสารที่ทำลายข้อจำกัดเดิม ทำให้ผู้รับสารสามารถเลือกรับสารตามความต้องการ โดยไม่มี

ข้อจำกัดทางด้านสถานที่ หรือเวลาเข้ามาเกี่ยวข้อง หรือเรียกอีกนัยหนึ่งว่าเป็นผู้รับสารที่สามารถแสวงหาหรือเลือกข้อมูลโดยเสรี (Active Sekker)

จึงสรุปได้ว่า การสื่อสารยุคดิจิทัล คือ กระบวนการสื่อความหมายผ่านสื่อดิจิทัล โดยมีองค์ประกอบสำคัญคือช่องทางการสื่อสาร ที่ทำให้ผู้รับสารมีอิทธิพลในการเลือกรับรู้เนื้อหาสารจากผู้ส่งสารโดยไม่มีตัวแปรทางด้านเวลาและกำหนดการเผยแพร่เนื้อหามาเกี่ยวข้อง

2.1.2 วัตถุประสงค์ของการสื่อสาร

มีหลากหลายคำนิยามเกี่ยวกับวัตถุประสงค์ของการสื่อสาร แต่โดยรวมกล่าวถึงวัตถุประสงค์ขั้นพื้นฐานเช่นเดียวกัน คือ การมีอิทธิพลต่อตนเอง ผู้อื่น รวมไปถึงสิ่งแวดล้อมโดยรอบ ทั้งนี้ก็เพื่อมุ่งหวังให้เกิดการเปลี่ยนแปลง ต่อทั้งความรู้ ทัศนคติ พฤติกรรม แม้กระทั่งก่อให้เกิดการเปลี่ยนแปลงทางด้านสิ่งแวดล้อม โดยสามารถสรุปวัตถุประสงค์ได้ดังตารางที่ 2.1 (Schramm, 1971 อ้างถึงใน อริสสา สชิลวิลเลอร์, 2559)

ตารางที่ 2.1 แสดงวัตถุประสงค์ของผู้รับสารและผู้ส่งสาร

วัตถุประสงค์ของผู้ส่งสาร	วัตถุประสงค์ของผู้รับสาร
1. เพื่อแจ้งให้ทราบ (To Inform) 2. เพื่อสอนหรือให้การศึกษา (To Educate) 3. เพื่อสร้างความพอใจหรือให้ความบันเทิง (To Entertain) 4. เพื่อเสนอหรือชักจูงใจ (To Persuade)	1. เพื่อทราบ (To Understand) 2. เพื่อศึกษา (To Learn) 3. เพื่อความพอใจ (To Enjoy) 4. เพื่อกระทำหรือตัดสินใจ (To Decide)

2.1.3 ประเภทของการสื่อสาร

ประเภทของการสื่อสาร สามารถจำแนกได้ทั้งหมด 3 ประเภท ได้แก่ จำแนกตามกระบวนการหรือการไหลของข่าวสาร จำแนกตามภาษาสัญลักษณ์ที่แสดงออก และ จำแนกตามจำนวนผู้สื่อสารซึ่งปรมะ สตะเวทิน (2546) ได้ให้คำอธิบายไว้ดังนี้

2.1.3.1 จำแนกตามกระบวนการหรือการไหลของข่าวสาร

1. การสื่อสารทางเดียว (One-way Communication)

เป็นการสื่อสารที่ข่าวสารจะถูกส่งออกจากผู้ส่งสารไปยังผู้รับสารในทิศทางเดียว โดยไม่มีการโต้ตอบจากผู้รับสาร เช่น การสื่อสารผ่านสื่อดั้งเดิม วิทยุ โทรทัศน์ หนังสือพิมพ์ รวมไปถึงการออกคำสั่งหรือมอบหมายงาน โดยที่ผู้รับไม่มีโอกาสได้แสดงความคิดเห็น ซึ่งอาจจะก่อให้เกิดความเข้าใจที่คลาดเคลื่อนกับวัตถุประสงค์ของการสื่อสารในครั้งนี้ การสื่อสารในลักษณะนี้จึงเหมาะสำหรับการสื่อสารในเรื่องที่เข้าใจง่าย

2. การสื่อสารสองทาง (Two-way Communication)

เป็นการสื่อสารที่มีการส่งข่าวสารออกจากผู้ส่งสารไปยังผู้รับสาร และมีการโต้ตอบไปกลับระหว่างผู้ส่งและผู้รับ ดังนั้นในการสื่อสารแต่ละครั้งแต่ละฝ่ายจึงทำหน้าที่เป็นทั้งผู้รับและผู้ส่งสารในขณะเดียวกัน การสื่อสารด้วยกระบวนการนี้จะทำให้ทราบผลของการสื่อสารอย่างทันท่วงทีว่าเข้าใจวัตถุประสงค์เดียวกันหรือไม่ ทั้งยังช่วยให้สามารถปรับวิธีการสื่อสารให้เหมาะสมกับแต่ละสถานการณ์ได้ เช่น การพูดคุยทางโทรศัพท์ การสั่งงานที่ผู้รับสามารถแสดงความคิดเห็นได้

2.1.3.2 จำแนกตามภาษาสัญลักษณ์ที่แสดงออก

1. การสื่อสารเชิงวัจนะ (Verbal Communication)

การสื่อสารโดยการใช้ภาษาพูด หรือบันทึกเป็นคำพูดในการสื่อสาร

2. การสื่อสารเชิงอวัจนะ (Non-Verbal Communication)

การสื่อสารโดยใช้รหัสสัญญาณที่ไม่ใช่การใช้ภาษาพูด เช่น ภาษากาย การแสดงออกทางใบหน้า สายตา น้ำเสียง ระดับเสียง หมายรวมถึงความเร็วในการพูด เป็นต้น

2.1.3.3 จำแนกตามจำนวนผู้สื่อสาร

1. การสื่อสารส่วนบุคคล (Intrapersonal Communication)

เป็นการสื่อสารที่นับรวม ความคิด การตัดสินใจของบุคคลใดบุคคลหนึ่ง ซึ่งจะแสดงพฤติกรรมออกมา เป็นกระบวนการที่เกิดขึ้นภายในบุคคล ซึ่งมีผลสะท้อนต่อบุคคลอื่นด้วย

2. การสื่อสารระหว่างบุคคล (Interpersonal Communication)

เป็นการสื่อสารที่มีจำนวนบุคคลในการสื่อสารตั้งแต่ 2 คนขึ้นไป เป็นการสื่อสารที่มีลักษณะตัวต่อตัว (Personal to Personal) เช่น การพูดคุยสนทนาระหว่าง 2 คน หมายรวมถึง การเขียนจดหมาย หรือการโทรศัพท์สนทนากัน

3. การสื่อสารมวลชน (Mass Communication)

เป็นการสื่อสารกับมวลชนจำนวนมากในเวลาเดียวกัน โดยอาศัยสื่อที่สามารถเข้าถึงได้ในระยะเวลาอันรวดเร็ว คือ สื่อมวลชน (Mass Media) อาทิ วิทยุ โทรทัศน์

2.1.4 แบบจำลองการสื่อสารของเบอร์โล

แบบจำลองการสื่อสารของเบอร์โล ประกอบด้วยองค์ประกอบสำคัญ 4 ประการ ได้แก่ ผู้ส่งสาร (Source) สาร (Messages) ช่องทาง (Channel) และ ผู้รับสาร (Receiver) ดังแสดงในตารางที่ 2.2

ตารางที่ 2.2 แบบจำลองการสื่อสารของเบอร์โล

ผู้ส่งสาร	สาร	ช่องทาง	ผู้รับสาร
1. ทักษะในการสื่อสาร 2. ความรู้ 3. ทัศนคติ 4. ระบบสังคม 5. วัฒนธรรม	1. รหัสสาร 2. เนื้อหาของสาร 3. การจัดเรียงลำดับสาร 4. องค์ประกอบย่อยของสาร 5. โครงสร้างสาร	1. การมองเห็น 2. การได้ยิน 3. การดมกลิ่น 4. การลิ้มรส 5. การสัมผัส	1. ทักษะในการสื่อสาร 2. ความรู้ 3. ทัศนคติ 4. ระบบสังคม 5. วัฒนธรรม

ดัดแปลงจากแบบจำลองการสื่อสารของเบอร์โล (Berlo, 1960)

เบอร์โล (Berlo, 1960) ให้คำอธิบายไว้ว่า ผลลัพธ์ของการสื่อสารจะมีประสิทธิภาพมากน้อยเพียงใด ขึ้นอยู่กับแต่ละองค์ประกอบ ซึ่งมีปัจจัยต่าง ๆ ที่เกี่ยวข้องดังต่อไปนี้

1. ผู้ส่งสาร (Source) จำเป็นจะต้องมีคุณสมบัติทั้ง 5 ประการ เพื่อให้การสื่อสารสามารถเป็นไปได้อย่างมีประสิทธิภาพสูงสุดดังนี้

1.1 ทักษะการสื่อสาร (Communication Skills) หมายถึง ความสามารถเกี่ยวกับการสื่อสารครบทุกด้าน ทั้งการพูด การอ่าน การฟัง รวมไปถึงการคิดไตร่ตรองโดยใช้เหตุผล

1.2 ความรู้ (Knowledge) หมายถึง ความรู้ลึกในประเด็นของสารที่ตนต้องการจะถ่ายทอดไปยังผู้รับสาร

1.3 ทัศนคติ (Attitude) หมายถึง ความโน้มเอียงในการเข้าถึงหรือหลีกเลี่ยง แบ่งเป็น 3 ประเภท ได้แก่ ทัศนคติต่อตนเอง เรื่องที่จะสื่อสาร และผู้รับสาร

1.4 ระบบสังคม (Social System) หมายถึง อิทธิของสังคมที่สามารถส่งผลต่อบุคคลและพฤติกรรมการสื่อสารได้

1.5 วัฒนธรรม (Culture) หมายถึง ขนบธรรมเนียม ประเพณี ค่านิยม และความเชื่อ ซึ่งเป็นตัวกำหนดรูปแบบการดำเนินชีวิต รวมถึงพฤติกรรมการสื่อสารของมนุษย์

2. สาร (Message) ผลลัพธ์ที่เกิดจากการเข้ารหัสของผู้ส่งสาร ซึ่งประกอบไปด้วย

2.1 รหัสของสาร (Messages Code) ได้แก่ ภาษา สัญลักษณ์ ท่าทาง ที่มนุษย์ใช้เพื่อแสดงออกแทนความรู้ ความคิด อารมณ์ รวมถึงความรู้สึกต่าง ๆ

2.2 เนื้อหาของสาร (Messages Content) หมายถึง องค์ความรู้ ความคิด และประสบการณ์ที่ผู้ส่งสาร ต้องการจะถ่ายทอดเรื่องราวต่าง ๆ เพื่อให้เกิดการรับรู้ร่วมกัน รวมถึงเพื่อเป็นการเลือกเปลี่ยนความเข้าใจหรือโต้ตอบกัน

2.3 การจัดสาร (Messages Treatment) หมายถึง การรวบรวมเนื้อหาของสารทั้งหมดแล้วนำมาเรียบร้อยเป็นระบบ เพื่อให้ได้ใจความตามเนื้อหา ที่ต้องการเลือก โดยใช้รหัสสารที่มีความเหมาะสม

3. ช่องทาง (Channel) นับได้ว่าเป็นองค์ประกอบที่มีความสำคัญ เนื่องจากเป็นสิ่งที่ทำหน้าที่นำสารจากผู้ส่งสาร ไปยังผู้รับสาร โดยสามารถแบ่งออกเป็น 3 ประเภท ดังนี้

3.1 ช่องสารที่นำสารจากผู้ส่งสารมายังผู้รับสาร อาทิ คลื่นแสง เสียง วิทยุ โทรทัศน์ หนังสือพิมพ์ และสื่อดิจิทัล เป็นต้น

3.2 ช่องสารที่เป็นพาหะนำสารไปสู่ประสาทรับรู้ทั้ง 5 อาทิ ได้ยิน ได้เห็น ได้กลิ่น ได้สัมผัส และได้ลิ้มรส

3.3 วิธีการเข้ารหัสและการถอดรหัส เช่น วิธีพูด หรือวิธีเขียนเป็นต้น

4. ผู้รับสาร (Receiver) จุดหมายปลายทางของการสื่อสาร ดังนั้นจึงจำเป็นจะต้องมีคุณสมบัติ 5 ประการเช่นเดียวกันกับผู้ส่งสาร

2.1.5 องค์ประกอบของการสื่อสารยุคดิจิทัล

วาสนา จันทร์สว่าง (2553 อ้างถึงใน อริสสา สชิวิลเลอร์, 2559) ให้คำอธิบายว่า การสื่อสารของมนุษย์ จะประกอบไปด้วยองค์ประกอบพื้นฐาน 4 ประการดังต่อไปนี้เสมอ

1. ผู้ส่งสารและผู้รับสาร การสื่อสารจะสัมฤทธิ์ผลได้นั้นทั้งผู้ส่งสารและผู้รับสารจะต้องสามารถตอบโต้สื่อสารกันได้ทั้งสองฝ่าย โดยจะต้องอยู่ในสภาวะแวดล้อมทางสังคมร่วมกัน มีสนามแห่งประสบการณ์ร่วม (Filed of Experience) หรือจำเป็นจะต้องมีความเข้าใจซึ่งกันและกัน

2. สาร คือสิ่งเร้าที่ผู้ส่งสารส่งออกไป โดยมีสารสนเทศเป็นเนื้อหาของสาร ซึ่งองค์ประกอบนี้มีความสำคัญอย่างยิ่งในบริบทการสื่อสารในสังคม เพราะหากมีสารสนเทศมากเพียงใด ก็สามารถทำให้การตัดสินใจเรื่องต่าง ๆ มีความถูกต้องและมีความเหมาะสมมากยิ่งขึ้น

3. สื่อหรือช่องทางการสื่อสาร เป็นตัวกลางที่จะนำสารจากผู้ส่งสารไปยังผู้รับสาร โดยจะต้องครอบคลุมประเด็นดังนี้

3.1 กลไกการรับรู้สาร คือ ผู้ส่งสารทำหน้าที่แปลงสัญญาณ หรือสัญลักษณ์ของสารส่งไปยังผู้รับสาร ส่วนการถอดรหัส คือการที่ผู้รับสารถอดความหมายจากสัญญาณหรือสัญลักษณ์ที่ผู้ส่งสารส่งมา

3.2 พาหะที่ทำให้สารเกิดการเคลื่อนไป มีช่องทางสำหรับนำสารไปสื่อประสาทสัมผัสทั้ง 5 ได้แก่ ได้ยิน ได้เห็น ได้กลิ่น ได้สัมผัส และได้ลิ้มรส

โดย ธนัท สมณคุปต์ (2562) ได้ขยายความเพิ่มเติมเกี่ยวกับประเภทของสื่อในองค์ประกอบการสื่อสารยุคดิจิทัลว่า เทคโนโลยีและนวัตกรรมช่วยเพิ่มประสิทธิภาพของ “สื่อ” ทำให้มนุษย์สามารถติดต่อสื่อสารกันได้อย่างรวดเร็ว ผ่านการใช้สื่อที่มีการนำข้อความ ภาพกราฟิก ภาพเคลื่อนไหว เสียงหรือวีดิทัศน์ มาร้อยเรียงผสมกัน จนเกิดเป็นสื่อที่มีความหลากหลายและเข้าถึงผู้รับสารได้ตรงกลุ่มเป้าหมายมากยิ่งขึ้น

2.1.6 สรุปแนวคิดเกี่ยวกับกระบวนการสื่อสารยุคดิจิทัล

การสื่อสารยุคดิจิทัล คือ กระบวนการเข้ารหัสและถอดรหัสสารระหว่างผู้ส่งสารและผู้รับสาร โดยผ่านช่องทางการสื่อสารสมัยใหม่ ที่อาศัยเทคโนโลยีและนวัตกรรมเข้าช่วยเพิ่มประสิทธิภาพ เพื่อให้เกิดความเข้าใจความหมายที่ถูกต้องร่วมกันทั้งสองฝ่าย โดยมีองค์ประกอบพื้นฐาน 4 ประการคือ ผู้ส่งสาร สาร ช่องทาง และ ผู้รับสาร ที่สำคัญประสิทธิผลของการสื่อสารจะขึ้นอยู่กับรายละเอียดของแต่ละปัจจัยที่กล่าวมาข้างต้น

ทั้งนี้ในการวิจัย ผู้วิจัยมุ่งศึกษา ปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล โดยประยุกต์ใช้แบบจำลองการสื่อสารข้างต้น มาเป็นกรอบในการศึกษาและอภิปรายผล เพื่อช่วยให้ผู้ศึกษาเข้าใจ และสามารถอธิบายถึงสาเหตุได้ชัดเจนมากยิ่งขึ้น

2.2 ทฤษฎีและแนวคิดเกี่ยวกับดิจิทัลเนทีฟ

2.2.1 ความหมายเกี่ยวกับดิจิทัลเนทีฟ

Mac Prensky (2001 อ้างถึงใน ณิศรา ศรีพลอยรุ่ง, 2558) ได้ให้คำนิยามไว้ว่า บุคคลที่เติบโตมาพร้อมกับเทคโนโลยี ทั้งคอมพิวเตอร์ วิดีโอเกม เครื่องเล่นเพลง กล้อง โทรศัพท์มือถือ และของเล่นอื่น ๆ โดยทั้งหมดนี้เกิดจากความรวดเร็วในการแพร่กระจายของเทคโนโลยีดิจิทัลในศตวรรษที่ 20

Toledo (2007 อ้างถึงใน ณิศรา ศรีพลอยรุ่ง, 2558) ให้ความหมายว่า เป็นบุคคลที่ผูกพันกับเทคโนโลยีใหม่

Palfrey and Gasser (2008 อ้างถึงใน สสินาท แสงทองฉาย, 2560) อธิบายว่า เป็นกลุ่มบุคคลที่สามารถผสานการใช้ชีวิตบนโลกของความจริง และบนโลกดิจิทัลได้อย่างไร้รอยต่อ ผ่านการทำกิจกรรมชีวิตประจำวัน การทำหลายสิ่งหลายอย่างในเวลาเดียวกัน รวมถึงการแสดงออกและความเชื่อมโยงกับบุคคลอื่น ๆ โดยใช้เทคโนโลยีดิจิทัล

Bennett (2012 อ้างถึงใน สสินาท แสงทองฉาย, 2560) อธิบายว่า Digital Native คือ ผู้เชี่ยวชาญการใช้เทคโนโลยี ซึ่งมีความสัมพันธ์กับช่องว่างดิจิทัล (Digital Divides)

ดารารัตน์ ภูธร (2561) ให้คำนิยามว่า เป็นชาวดิจิทัลโดยกำเนิด สามารถใช้อุปกรณ์คอมพิวเตอร์ อินเทอร์เน็ต และอุปกรณ์ดิจิทัลได้อย่างชำนาญ

จึงสรุปได้ว่า ดิจิทัลเนทีฟ (Digital Native) คือ บุคคลที่เป็นชาวดิจิทัลโดยกำเนิด สามารถใช้งานอุปกรณ์รวมถึงเทคโนโลยีต่าง ๆ เพื่อติดต่อสื่อสาร ทำกิจกรรมในชีวิตประจำวันได้อย่างชำนาญ

2.2.2 ดิจิทัลเนทีฟและดิจิทัลอิมมิแกรนท์

นอกจากนี้การศึกษาของ Mac Prensky (2001) ยังชี้ให้เห็นว่า บุคคลที่เป็นดิจิทัลเนทีฟจะมีทักษะความสามารถประหนึ่งเป็นเจ้าของภาษา (Native Speaker) ของภาษาดิจิทัล ทำให้สามารถรับรู้ข้อมูลข่าวสารได้อย่างรวดเร็ว ทั้งยังสามารถทำกิจกรรมบนโลกออนไลน์ได้หลายอย่างพร้อมกัน นอกจากนั้นกลุ่มคนดิจิทัลเนทีฟยังนิยมข้อมูลที่เป็นภาพกราฟิกก่อนตัวอักษร นอกจากนี้ Mac Prensky ยังได้กล่าวถึงบุคคลที่ไม่ได้เกิดมาพร้อมกับโลกของดิจิทัล ได้แต่รับอิทธิพลในภายหลัง และมีการปรับเปลี่ยนสภาพแวดล้อมให้เข้ากับเทคโนโลยีในปัจจุบัน โดยเรียกกลุ่มคนเหล่านี้ว่า ดิจิทัลอิมมิแกรนท์ (Digital Immigrant)

ทั้งนี้ Vamslyke (2003 อ้างถึงใน ศุภกร จูฑะพล, 2557) ได้ศึกษาแนวคิดของ Mac Prensky เพิ่มเติมพบว่า นิยามของ Digital Natives และ Digital Immigrants เป็นเพียงนิยามเชิงแนวคิดเท่านั้น เนื่องจากไม่ได้กล่าวถึงช่วงอายุที่แน่นอน กระทั่งสหภาพโทรคมนาคมระหว่างประเทศ ITU (2013) ได้ทบทวนแนวคิด และงานวิจัยที่เกี่ยวข้อง ทำให้ทราบข้อมูลเชิงลึกว่า เกณฑ์ในการจำแนกระหว่าง Digital Native และ Digital Immigrants มีความเกี่ยวข้องกับคุณลักษณะของช่วงอายุ เจเนอเรชัน ปีเกิด ระดับของการเปิดรับอินเทอร์เน็ต ความลึกซึ้งในการใช้งานเทคโนโลยีทั้งความลึกและความกว้าง ระดับรายได้ ความถี่ ความเชี่ยวชาญ และระดับสติปัญญาในการเรียนรู้ เป็นต้น ซึ่งตัวชี้วัดเหล่านี้ก่อให้เกิดความยากลำบากในการกำหนดนิยาม ITU (2013 อ้างถึงใน ศุภกร จูฑะพล, 2557) จึงกำหนดนิยามใหม่ ที่มีความเป็นสากลมากที่สุดเพื่อใช้ในการวิจัยทั่วโลก โดยนำช่วงอายุที่พบจากงานวิจัยมากที่สุดมาเฉลี่ยเป็นเกณฑ์ตั้งต้น พร้อมทั้งระบุประสบการณ์ในการใช้งานอินเทอร์เน็ตอย่างต่ำ 5 ปี เป็นตัวชี้วัดบอกถึงการเข้าถึงดิจิทัล ในส่วนของตัวชี้วัดที่ยากจะสามารถวัดผลได้ อาทิ ความลึก และความแตกต่างสติปัญญา จะไม่ถูกนำมาเป็นตัวชี้วัดในครั้งนี้ ITU จึงกำหนดนิยามแรกของ Digital Natives ว่าเป็นเยาวชนผู้มีอายุ 15-24 ปี และมีประสบการณ์ในการใช้งานอินเทอร์เน็ตอย่างต่ำ 5 ปีขึ้นไป

จากนิยามดังกล่าว ทำให้ทราบว่า Digital Natives คือเยาวชนที่มีอายุระหว่าง 15-24 ปี เป็นผู้ที่เกิดในช่วงปี พ.ศ. 2532-2541 (คำนวณจากปีที่เผยแพร่เอกสาร) ซึ่งมีช่วงของอายุที่คาบเกี่ยวระหว่างเจเนอเรชัน Y (พ.ศ. 2523-2540) และเจเนอเรชัน Z (ผู้ที่เกิด พ.ศ. 2541 เป็นต้นไป) (มนัสวี ศรีนนท์, 2561) โดยนิยามที่ ITU กำหนด ผู้วิจัยเลือกมาใช้ในการศึกษาวิจัยเรื่อง การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล

O. Zur และ A. Zur (2011) ยังได้ทำการเปรียบเทียบความแตกต่างของคุณลักษณะของดิจิทัลเนทีฟ และดิจิทัลอิมมิแกรนท์ โดยมีพื้นฐานมาจากงานวิจัยของ Rosen (2011 อ้างถึงในวณิศรา ศรีพลอยรุ่ง, 2558) ซึ่งแสดงความแตกต่างดังเปรียบเทียบในตารางที่ 2.3

ตารางที่ 2.3 ความแตกต่างของคุณลักษณะของดิจิทัลเนทีฟและดิจิทัลอิมมิแกรนท์

ดิจิทัลเนทีฟ (Digital Natives)	**ดิจิทัลอิมมิแกรนท์ (Digital Immigrants)**
พฤติกรรมการสื่อสารผ่านสื่อดิจิทัล	
1. ชอบการติดต่อผ่านตัวอักษร แชท และเกมออนไลน์ 2. ใช้สำหรับส่งข้อความตัวอักษรมากกว่าการโทรศัพท์ 3. ชอบการสื่อสารที่เป็นลำดับ เช่น อีเมล เฟซบุ๊ก หรือการแชท 4. ชอบการรับข้อมูลข่าวสารอย่างรวดเร็ว จากหลาย ๆ สื่อพร้อมกัน และจะเลือกรับข้อมูลมากกว่า 1 แหล่ง 5. ใช้ตัวอักษรย่อในการพิมพ์ส่งข้อความ เช่น cu tomorrow	1. ชอบพูดคุยผ่านทางโทรศัพท์ หรือสนทนาโดยเห็นหน้าค่าตามากกว่า 2. ไม่นิยมในการพิมพ์ส่งข้อความ หรือจะใช้น้อย และใช้ด้วยความไม่เต็มใจ 3. ชอบการสื่อสารที่เป็นแบบเรียลไทม์ เช่นการคุยต่อหน้า หรือโทรศัพท์ 4. ชอบรับข้อมูลข่าวสารอย่างช้า ๆ เป็นลำดับขั้นตอน เป็นเส้นตรง ตามเหตุและผล 5. ให้ความสำคัญกับการใช้ถ้อยคำที่ถูกต้อง ในการพิมพ์บทสนทนา

ตารางที่ 2.3 ความแตกต่างของคุณลักษณะของดิจิทัลเนทีฟและดิจิทัลอิมมิแกรนท์ (ต่อ)

ดิจิทัลเนทีฟ (Digital Natives)	ดิจิทัลอิมมิแกรนท์ (Digital Immigrants)
พฤติกรรมการสื่อสารผ่านสื่อดิจิทัล (ต่อ)	
6. ชื่นชอบการเล่าเรื่องราวเกี่ยวกับทริปการเดินทางผ่านภาพถ่ายและข้อความลงในเฟซบุ๊ก 7. รับรู้เรื่องราวและข่าวสารจากเพื่อน (ฟีดเฟซบุ๊ก) ทวิตเตอร์ บล็อก ทั้งยังมองว่าสื่อดั้งเดิม ไม่ใช่ศูนย์กลางข่าวสาร	6. ชื่นชอบการเล่าเรื่องราวเกี่ยวกับทริปการเดินทาง โดยการโทรบอกหรือเปิดรูปถ่ายให้คนอื่นชม 7. รับรู้ข่าวสารจากสื่อดั้งเดิม เช่น หนังสือพิมพ์ นิตยสาร (นิยมอ่านหนังสือแบบเป็นเล่ม)
คุณลักษณะด้านรูปแบบการดำเนินชีวิต	
8. ไม่สามารถใช้คู่มือ มักเรียนรู้และแก้ไขปัญหาโดยใช้สัญชาตญาณตน ชอบค้นพบอะไรใหม่ ๆ โดยการทดลองมากกว่าพิจารณาไตร่ตรอง 9. ชอบทำกิจกรรม หรือทำงานหลาย ๆ อย่างไปพร้อมกัน หรือสลับไปมา 10. ชอบที่จะมีงาน และสร้างสรรค์กิจกรรมใหม่ ๆ ขึ้นมาเสมอ 11. ชอบการมีปฏิสัมพันธ์กับ ภาพ เสียง กราฟิก วิดีโอมากกว่าข้อความ 12. มีแนวโน้มอ่านหนังสือได้น้อยลง และสลับทำกิจกรรมอย่างอื่นแทน 13. พึงพอใจในความเร็ว ไม่เห็นคุณค่าของการรอ	8. คุ้นเคยกับคู่มือที่บอกลำดับ ขั้นตอนการจัดการ เป็นนักเรียนรู้ที่พิจารณาไตร่ตรอง มีเหตุมีผล และจะปฏิบัติตามเป็นลำดับเส้นตรง 9. ชอบทำกิจกรรมอย่างเดียว ไม่ชอบทำหลาย ๆ กิจกรรม ในเวลาเดียวกัน 10. มีความพึงพอใจกับงานหรือกิจกรรมเพียงอย่างเดียวที่ทำในขณะนั้น 11. ชอบการอ่านข้อความยาว ๆ เช่น อ่านหนังสือ มากกว่าภาพ วิดีโอ 12. มีแนวโน้มที่จะอ่านหนังสือแบบละเอียดถี่ถ้วน 13. เห็นคุณค่าของความพึงพอใจที่จะต้องรอคอย

ตารางที่ 2.3 ความแตกต่างของคุณลักษณะของดิจิทัลเนทีฟและดิจิทัลอิมมิแกรนท์ (ต่อ)

ดิจิทัลเนทีฟ (Digital Natives)	ดิจิทัลอิมมิแกรนท์ (Digital Immigrants)
คุณลักษณะด้านรูปแบบการดำเนินชีวิต (ต่อ)	
14. มีการติดต่อเพื่อนผ่านทั้งช่องทางออนไลน์ (โซเชียลมีเดีย) และออฟไลน์ (อีเวนต์ต่าง ๆ) ไปพร้อมกัน	14. มีการติดต่อกับเพื่อน ผ่านกิจกรรมสังสรรค์ ไปพบที่คลับ หรือทานอาหารค่ำร่วมกัน
คุณลักษณะด้านมุมมองเกี่ยวกับการทำงาน	
15. มีมุมมองการทำงานว่า ทุกคนมีความเท่าเทียมกัน 16. ทำงานและพักไปพร้อมกัน ไม่ยึดติดว่าจะต้องพักผ่อนในวันหยุดเท่านั้น 17. จะพยายามทำหลากหลายอาชีพ สลับปรับเปลี่ยนหน้าที่ทำงานไปเรื่อย ๆ ไม่คำนึงถึงความปลอดภัย มั่นคง มากกว่าการได้ประสบการณ์ 18. นึกถึงความพึงพอใจส่วนบุคคลมากกว่าองค์กร การเปลี่ยนงานบ่อย ๆ จะพัฒนาเป็นการพัฒนาทักษะความสามารถของตนเอง 19. ชอบการสื่อสารทางไกล และชั่วโมงการทำงานที่ยืดหยุ่นได้ 20. ชอบการสลับความสนใจไปมาระหว่างการทำงานและกิจกรรมบนโลกออนไลน์	15. มีมุมมองการทำงานที่ให้ความสำคัญเรื่องลำดับชั้น มากกว่าความเท่าเทียมหรือประชาธิปไตย 16. มีความยึดมั่นในการทำงานติดต่อกัน 5 วัน และจะพักในวันหยุดเท่านั้น 17. มีค่านิยมในการทำงานที่ยึดมั่นกับบริษัท อาชีพเดียวตลอดชีวิต เลื่อนตำแหน่งขึ้นไปเรื่อย ๆ ถึงเวลาก็เกษียณรับเงินบำเหน็จ บำนาญ 18. มีค่านิยมที่จะภักดีต่อบริษัทที่ตนเองทำงานอยู่ มั่นคงไม่เปลี่ยนแปลง รวมถึงมีแนวโน้มที่จะไม่ย้ายไปทำงานที่อื่น 19. ชอบการทำงานอยู่แต่ในบริษัท ไม่ค่อยเชื่อใจในการสื่อสารทางไกล 20. หากเป็นชั่วโมงทำงาน ก็จะทำงานอย่างจริงจัง

ตารางที่ 2.3 ความแตกต่างของคุณลักษณะของดิจิทัลเนทีฟและดิจิทัลอิมมิแกรนท์ (ต่อ)

ดิจิทัลเนทีฟ (Digital Natives)	ดิจิทัลอิมมิแกรนท์ (Digital Immigrants)
คุณลักษณะด้านมุมมองที่มีต่ออินเทอร์เน็ต	
21. ใช้อินเทอร์เน็ตเพื่อติดต่อกับเพื่อน พร้อมทั้งใช้เพื่อความบันเทิงต่าง ๆ 22. มองอินเทอร์เน็ตว่าเป็นเครื่องมือในการสร้างปฏิสัมพันธ์มากกว่าการรับข้อมูลเพียงด้านเดียว 23. มีมุมมองที่หลากหลายของชีวิต ซึ่งเกิดขึ้นเพราะการใช้งานอินเทอร์เน็ต 24. อินเทอร์เน็ตคือความจริง จับต้องได้มากกว่าชีวิตจริงบนโลกออฟไลน์ 25. ไม่ค่อยคำนึงถึงความเป็นส่วนตัว มักเผยข้อมูลส่วนบุคคลลงบนโลกออนไลน์	21. ใช้อินเทอร์เน็ตเป็นเพียงแหล่งรวบรวมข้อมูลต่าง ๆ 22. มองอินเทอร์เน็ตเป็นเพียงช่องทางการสื่อสารทางเดียว และใช้งานเพื่อ อ่าน รับข้อมูล และเรียนรู้ 23. มองว่าเด็กและเยาวชน เสียเวลาชีวิตไปกับโลกออนไลน์ 24. มองว่าอินเทอร์เน็ตเป็นเพียงโลกเสมือน ไม่ใช่โลกของความจริง 25. ให้ความสำคัญกับการรักษาความเป็นส่วนตัว และเผยข้อมูลบางส่วนเท่านั้น
คุณลักษณะด้านการเรียนรู้	
26. ชอบเรียนรู้เท่าที่จำเป็นจะต้องรู้ 27. การเรียนรู้ ควรผสมผสานความสนุกสนานเข้าไปด้วย	26. ชอบเรียนรู้แบบเผื่อเอาไว้ 27. การเรียนรู้เป็นสิ่งจำเป็น และเป็นงานหนักที่เลี่ยงไม่ได้
คุณลักษณะด้านการมีปฏิสัมพันธ์กับผู้อื่น	
28. ชอบปฏิสัมพันธ์กับผู้คนที่หลากหลายมากกว่าการมีเพื่อนสนิทจำกัดเพียง 29. ปฏิสัมพันธ์ที่มีคุณภาพสามารถเกิดขึ้นได้ ผ่านเครือข่ายสังคมออนไลน์ สามารถสนิทสนมกันได้ง่าย	28. ชอบการมีปฏิสัมพันธ์ที่มีคุณภาพกับคนสนิทเพียงไม่กี่คน 29. ปฏิสัมพันธ์ที่มีคุณภาพได้จะเกิดขึ้นกับเพื่อนที่ตนสนิทเพียงเท่านั้น ซึ่งรู้จัก และมีความไว้เนื้อเชื่อใจกัน

ตารางที่ 2.3 ความแตกต่างของคุณลักษณะของดิจิทัลเนทีฟและดิจิทัลอิมมิแกรนท์ (ต่อ)

ดิจิทัลเนทีฟ (Digital Natives)	ดิจิทัลอิมมิแกรนท์ (Digital Immigrants)
คุณลักษณะด้านการมีปฏิสัมพันธ์กับผู้อื่น (ต่อ)	
30. มีความกังวลถึงความปลอดภัย ในการส่งภาพเปลือย การคุกคามเกาะติดชีวิตผู้อื่นบนโลกไซเบอร์ (Cyber stalking) การรังแกบนโลกออนไลน์ (Cyberbullying) รวมถึงการบุกรุกความเป็นส่วนตัว	30. มีความกังวลแบบดั้งเดิม ในเรื่องของการลักพาตัว การข่มขืน การถูกปล้นชิงทรัพย์ เป็นต้น

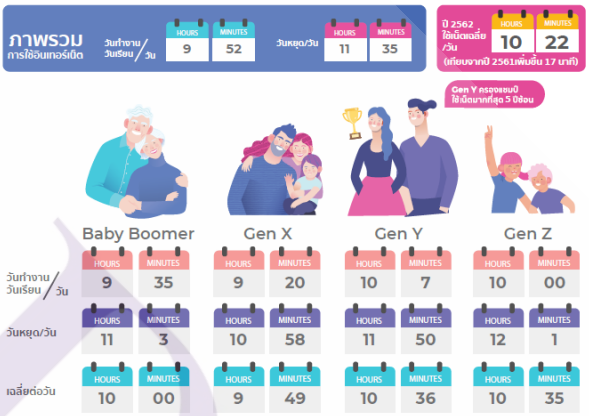
ที่มา: Rosen (2011 อ้างถึงใน วณิศรา ศรีพลอยรุ่ง, 2558)

สรุปได้ว่า กลุ่มดิจิทัลเนทีฟ จะมีการใช้งานสื่อดิจิทัลที่คล่องกว่า ทั้งยังมีแนวคิด วิธีการดำเนินชีวิต ลักษณะการทำงาน ความซื่อสัตย์ต่อองค์กร รูปแบบการเรียนรู้ การใช้ชีวิตในสังคม เรื่องการพูดคุยกับบุคคลแปลกหน้า รวมถึงการตระหนักรู้เรื่องความปลอดภัยบนโลกออนไลน์ ที่ต่างจากกลุ่มดิจิทัลอิมมิแกรนท์ ที่ยังคงยึดถือแนวคิด วิธีการมีปฏิสัมพันธ์ หรือภัยร้ายบนโลกออฟไลน์เช่นเดิม

2.2.3 คุณลักษณะและการใช้สื่อของดิจิทัลเนทีฟไทย

งานวิจัยของ ITU (2013 อ้างถึงใน ศุภกร จูฑะพล, 2557) ได้จัดอันดับกลุ่มคนดิจิทัลเนทีฟของประเทศไทยอยู่ลำดับที่ 85 จาก 180 ประเทศทั่วโลก ซึ่งมีจำนวนทั้งสิ้น 4,387,062 คน หรือคิดเป็น 6.3 ของจำนวนประชากรทั้งประเทศ โดยส่วนใหญ่เป็นเยาวชนที่มีอายุระหว่าง 15-24 ปี คิดเป็นร้อยละ 42.3 จากจำนวนดิจิทัลเนทีฟทั่วประเทศไทย นอกจากนี้ไมล์แชร์ (2014) เอเจนซี่ด้านการสื่อสารและการตลาดของประเทศไทย ได้เผยผลการวิจัยเรื่อง “Growing Up as Digital Natives” พบว่าผู้ใช้อินเทอร์เน็ตในประเทศไทย มีจำนวนทั้งสิ้น 16,284,000 คน ซึ่งมากกว่าครึ่งของผู้ใช้เป็นบุคคลกลุ่มดิจิทัลเนทีฟ จำนวน 8,570,890 คน

นอกจากนี้จากรายงานผลสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2562 ซึ่งสำรวจโดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร พบว่าเจเนอเรชันวาย หรือบุคคลที่เกิดในปี พ.ศ. 2524 – 2543 (อายุระหว่าง 20-39 ปี) จะเป็นกลุ่มคนที่เติบโตมาพร้อมกับเทคโนโลยีดิจิทัล จึงส่งผลให้มีปริมาณการใช้งานอินเทอร์เน็ตที่สูงกว่าคนในเจนอื่น

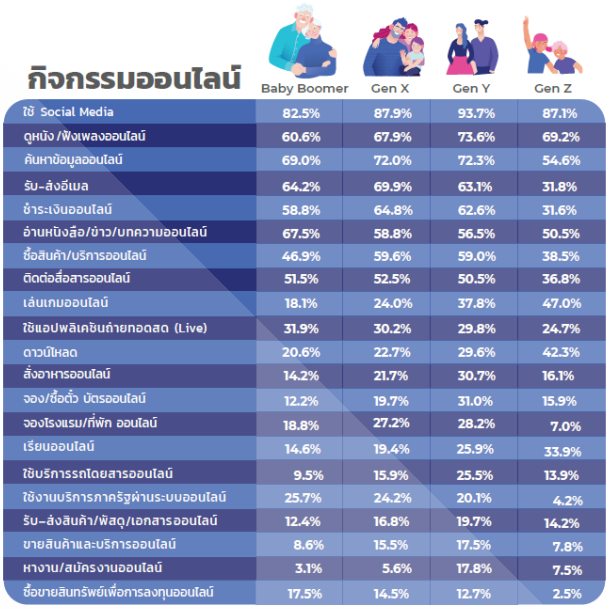


ภาพที่ 2.1 จำนวนชั่วโมงการใช้อินเทอร์เน็ตโดยเฉลี่ยต่อวัน ในแต่ละเจนเนอเรชัน

ที่มา: รายงานผลสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2562 โดย สพธอ (2562)

จากสถิติข้างต้นจะพบว่า เมื่อจำแนกตามเจนเนอเรชัน กลุ่มเจนวายจะมีการใช้งานอินเทอร์เน็ตสูงที่สุด จำนวน 10 ชั่วโมง 36 นาที รองลงมาคือเจนซีจำนวน 10 ชั่วโมง 35 นาที เบบี้บูมเมอร์ จำนวน 10 ชั่วโมง และ เจนเอ็กซ์ จำนวน 9 ชั่วโมง 49 นาที

นอกจากนี้ยังพบว่ากลุ่มเจนวาย นิยมใช้อินเทอร์เน็ตเพื่อติดต่อสื่อสารผ่านช่องทางโซเชียลมีเดีย ใช้สำหรับดูหนังฟังเพลงออนไลน์ ค้นหาข้อมูล รวมไปถึงรับส่งอีเมลออนไลน์



กิจกรรมออนไลน์	Baby Boomer	Gen X	Gen Y	Gen Z
ใช้ Social Media	82.5%	87.9%	93.7%	87.1%
ดูหนัง/ฟังเพลงออนไลน์	60.6%	67.9%	73.6%	69.2%
ค้นหาข้อมูลออนไลน์	69.0%	72.0%	72.3%	54.6%
รับ-ส่งอีเมล	64.2%	69.9%	63.1%	31.8%
ชำระเงินออนไลน์	58.8%	64.8%	62.6%	31.6%
อ่านหนังสือ/ข่าว/บทความออนไลน์	67.5%	58.8%	56.5%	50.5%
ซื้อสินค้า/บริการออนไลน์	46.9%	59.6%	59.0%	38.5%
ติดต่อสื่อสารออนไลน์	51.5%	52.5%	50.5%	36.8%
เล่นเกมออนไลน์	18.1%	24.0%	37.8%	47.0%
ใช้แอปพลิเคชันถ่ายทอดสด (Live)	31.9%	30.2%	29.8%	24.7%
ดาวน์โหลด	20.6%	22.7%	29.6%	42.3%
สั่งอาหารออนไลน์	14.2%	21.7%	30.7%	16.1%
จอง/ซื้อตั๋ว บัตรออนไลน์	12.2%	19.7%	31.0%	15.9%
จองโรงแรม/ที่พัก ออนไลน์	18.8%	27.2%	28.2%	7.0%
เรียนออนไลน์	14.6%	19.4%	25.9%	33.9%
ใช้บริการรถโดยสารออนไลน์	9.5%	15.9%	25.5%	13.9%
ใช้งานบริการภาครัฐผ่านระบบออนไลน์	25.7%	24.2%	20.1%	4.2%
รับ-ส่งสินค้า/พัสดุ/เอกสารออนไลน์	12.4%	16.8%	19.7%	14.2%
ขายสินค้าและบริการออนไลน์	8.6%	15.5%	17.5%	7.8%
หางาน/สมัครงานออนไลน์	3.1%	5.6%	17.8%	7.5%
ซื้อขายสินทรัพย์เพื่อการลงทุนออนไลน์	17.5%	14.5%	12.7%	2.5%

ภาพที่ 2.2 กิจกรรมการใช้งานผ่านอินเทอร์เน็ต ในแต่ละเจนเนอเรชัน

ที่มา: รายงานผลสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2562 โดย สพธอ (2562)

จากสถิติและข้อมูลข้างต้น จะเห็นได้ว่ากลุ่มบุคคลดิจิทัลเนทีฟที่มีอายุระหว่าง 18-36 ปี มีความสามารถในการเข้าถึงอุปกรณ์ เทคโนโลยีดิจิทัล รวมถึงอินเทอร์เน็ตได้ในระดับที่สูง ทั้งยังมีพฤติกรรมการติดต่อสื่อสารผ่านช่องทางออนไลน์ มีการรับส่งอีเมล

ด้วยเหตุนี้งานวิจัย การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล จึงกำหนดนิยามเชิงปฏิบัติการให้กลุ่มบุคคลผู้รับสารที่เป็นดิจิทัลเนทีฟไทย เป็นผู้อยู่ในช่วงอายุ 18-36 ปี เนื่องจากมีความสามารถในการใช้งานอุปกรณ์ เทคโนโลยีดิจิทัล รวมถึงสามารถใช้งานอินเทอร์เน็ตได้เป็นอย่างดี ซึ่งนับได้ว่าเป็นปัจจัยสำคัญที่จะทำให้บุคคลเหล่านี้มีโอกาสในการประสบพบเจอกับการถูกล่อลวงมากกว่าวัยอื่น

2.3 การถูกล่อลวงบนสื่อดิจิทัล

2.3.1 สื่อดิจิทัล

สื่อดิจิทัล คือ เครื่องมือในการสื่อสาร ที่สามารถผสมผสานระหว่างตัวอักษร ภาพนิ่ง เสียง ภาพเคลื่อนไหว โดยใช้เทคโนโลยีอินเทอร์เน็ตเป็นตัวกลางสำคัญในการรวมการสื่อสาร

ระหว่างโปรแกรมต่าง ๆ อาทิ เฟซบุ๊ก ทวิตเตอร์ อีเมล เป็นต้น (เอมิการ์ ศรีธาตุ, 2559) โดยนำข้อมูลข้างต้นมาแปลงสภาพ และเชื่อมโยงเข้าด้วยกันเพื่อประโยชน์ในการใช้งาน โดยอาศัยเทคโนโลยีและความเจริญก้าวหน้าทางด้านระบบเครือข่ายอินเทอร์เน็ตเข้าช่วย

โดยทั่วไปสื่อดิจิทัลมีองค์ประกอบ 5 ชนิดดังนี้ (ธันยวิช วิเชียรพันธ์, 2557 อ้างถึงใน เอมิการ์ ศรีธาตุ, 2559)

1. ข้อความ (Text) เป็นส่วนประกอบของเนื้อหา มีรูปแบบของตัวอักษรและสีของตัวอักษร สามารถกำหนดคุณลักษณะให้เข้ากับรูปแบบในการนำเสนอแต่ละครั้งได้

2. เสียง (Audio) จัดเก็บไฟล์ในลักษณะของสัญญาณดิจิทัล สามารถเล่นซ้ำได้โดยใช้โปรแกรม โดยเสียงจะมีความน่าสนใจมากยิ่งขึ้น เมื่อใช้ประกอบกับสื่อผสมอย่างอื่น

3. ภาพนิ่ง (Still Images) ใช้ถ่ายทอดการรับรู้ และสื่อสารความหมายต่าง ๆ ทำให้เข้าใจบริบทของสื่อนั้น ๆ ได้เช่นเจนมากยิ่งขึ้น

4. ภาพเคลื่อนไหว (Animation) เป็นภาพกราฟิกที่มีคุณลักษณะพิเศษ คือสามารถเคลื่อนไหวได้ ทำให้สร้างจินตนาการแก่ผู้รับสาร ก่อให้เกิดแรงจูงใจได้ดีกว่าสื่อประเภทภาพนิ่ง

5. ภาพวิดีโอ (Video) เป็นองค์ประกอบที่สำคัญมาก เนื่องจากเป็นการผสมผสานสื่อทั้ง 4 ชนิด อันได้แก่ ข้อความ เสียง ภาพนิ่ง และภาพเคลื่อนไหว เข้าด้วยกันอย่างสมบูรณ์

สื่อดิจิทัลจึงมีบทบาทสำคัญที่ใช้ในการสื่อสารในปัจจุบัน โดย Kaul (2012 อ้างถึงใน วิทวัฒน์ ฉุยกลัด, 2558) ได้ให้คำนิยามของการสื่อสารดิจิทัลว่า เป็นพลังที่นำการเปลี่ยนแปลงที่ยิ่งใหญ่ นับจากยุคปฏิวัติอุตสาหกรรม ซึ่งจะเป็นดังพลังของคลื่นสึนามิ ที่ทำให้เกิดการเปลี่ยนแปลงภูมิทัศน์ทางสังคม

การสื่อสารดิจิทัลมีคุณลักษณะสำคัญ 5 ประการ คือ ความเป็นดิจิทัล การหลอมรวมการมีปฏิสัมพันธ์ การเชื่อมโยง และประสบการณ์เสมือน (Flew, 2005; Lister et al., 2009; Chen and Zhang, 2010 อ้างถึงใน วิทวัฒน์ ฉุยกลัด, 2558)

1. ความเป็นดิจิทัล ถือเป็นคุณสมบัติเด่น เนื่องจากสามารถผสมผสานภาพ เสียงต่าง ๆ ที่แปลงจากระบบ Analog เป็น Digital ซึ่งทำงานด้วยวิธีการทางคณิตศาสตร์ (Mathematical Operations) ทำให้สามารถที่จะดำเนินการควบคุม จัดเก็บ และนำมาใช้ซ้ำได้

2. พลังงานหลอมรวม ทำให้ง่ายต่อการส่งต่อผ่านทางอินเทอร์เน็ต และก่อให้เกิดความสะดวกในการจัด รวม ทั้งผลผลิตและการบริการไว้ด้วยกัน

3. การปฏิสัมพันธ์ ได้สร้างอิสรภาพอันยิ่งใหญ่ในการผลิต และการผลิตซ้ำเนื้อหา ทำให้ผู้ใช้กับทรัพยากรข้อมูล สามารถติดต่อสื่อสารกันได้

4. การเชื่อมโยง ทำให้คนทั้งโลกสามารถเชื่อมโยงกันได้ และนำไปสู่การเปลี่ยนแปลงกิจกรรมทางการเงิน เปลี่ยนวิถีชีวิตและมิติอื่น ๆ ของผู้คนในสังคม

5. ประสบการณ์เหมือน สร้างช่องว่างระหว่างความจริงและโลกเสมือน ซึ่งมีผลต่อเพศสภาพ บุคลิกภาพ อาชีพ ก่อเกิดชุมชน สังคมเสมือนมากมาย

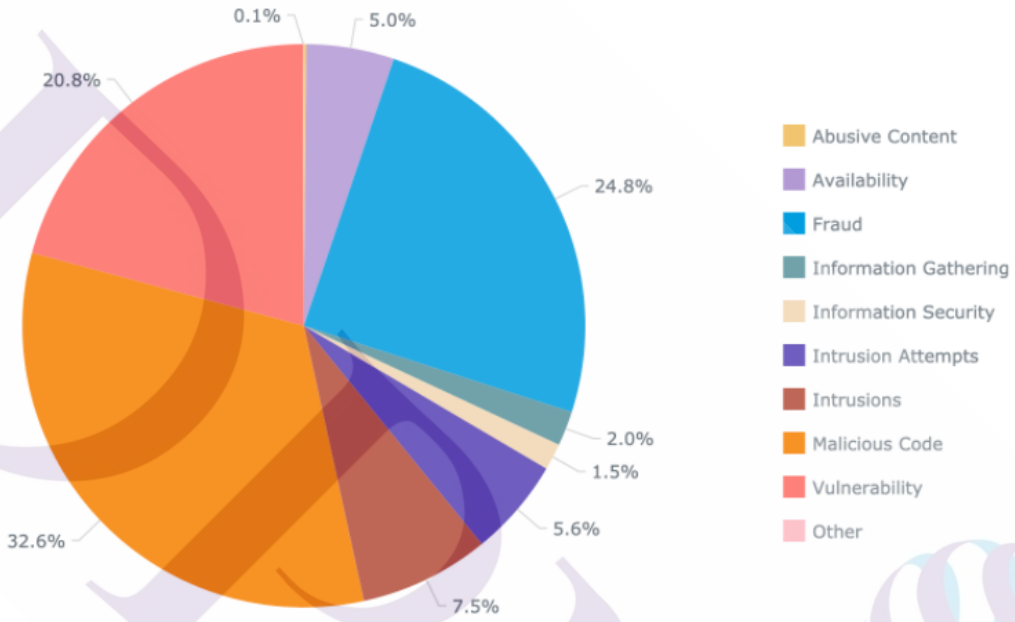
ดังนั้นสรุปได้ว่าการสื่อสารดิจิทัล คือ การผสมผสานการสื่อสารในรูปแบบดั้งเดิมทั้งตัวอักษร ภาพ เสียง แสดงผลด้วยกรรมวิธีสมัยใหม่ พร้อมทั้งจัดเก็บ และส่งต่อโดยมีเทคโนโลยีดิจิทัลเข้ามาเกี่ยวข้อง

2.3.2 การล่อลวงบนสื่อดิจิทัล

การล่อลวงบนสื่อดิจิทัล นับได้ว่าเป็นหนึ่งในอาชญากรรมคอมพิวเตอร์ประเภทการฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ที่มีวัตถุประสงค์ในการลักลอบขโมยข้อมูลสำคัญของผู้เสียหาย เช่น ชื่อผู้ใช้ รหัสผ่าน รหัสบัตรเครดิต หรือข้อมูลสำหรับทำธุรกรรมทางอิเล็กทรอนิกส์ (กุลธิดา อาธิเจริญสุข, 2559) ให้ความหมายไว้ว่า เป็นการล่อลวงให้ผู้เสียหายใช้บริการของระบบที่ปลอมแปลงขึ้น โดยที่ผู้เสียหายไม่ทราบว่าระบบที่ตนกำลังใช้งานอยู่นั้นเป็นระบบที่ถูกปลอมแปลงโดยมีศัพท์ทางเทคนิคเรียกวิธีการโจมตีในลักษณะนี้ว่า ฟิชชิ่ง (Phishing) การปลอมแปลงระบบที่เกิดขึ้นไม่ได้จำกัดอยู่แค่เฉพาะการส่งอีเมลเท่านั้น ยังสามารถส่งระบบปลอมโดยใช้ลิงก์ URL ไปยังช่องทางอื่น ๆ อาทิ การส่งข้อความผ่านสื่อโซเชียลมีเดีย การส่งข้อความสั้น (SMS) หรือการโทรหลอกลวงผ่านโทรศัพท์ ฟิชชิ่ง จึงจัดเป็นหนึ่งในภัยคุกคามด้านการโจมตีด้วยวิธีวิศวกรรมสังคม (Social Engineering) ซึ่งใช้หลักจิตวิทยา ความไม่รู้ หรือความประมาทของเหยื่อ ลอกเลียนแบบหรือองค์กรที่น่าเชื่อถือให้เหยื่อเกิดพฤติกรรมอันตรายขึ้น

โดยศูนย์ประสานงานรักษาความมั่นคงระบบคอมพิวเตอร์ (ไทยเซิร์ต, 2563) รายงานว่าคนไทยเสี่ยงต่อการถูกโจมตีประเภท Malicious Code การติดตั้งโปรแกรมที่มีคำสั่งอันตรายมากที่สุด ตามด้วย Fraud คือการปลอมตัวเป็นนิติบุคคลอื่น (WP4 Clearinghouse Policy, 2003) โดยนิยม

ใช้วิธีที่เรียกว่า ฟิชชิ่ง (Phishing) ซึ่งมักจะปลอมแปลงเป็นบุคคล หน่วยงาน หรือแหล่งข้อมูลที่น่าเชื่อถือส่ง URL ให้เหยื่อคลิก เข้าถึง และกรอกข้อมูล โดยการทำฟิชชิ่งยังสามารถโจมตีผ่านทางช่องทางอื่น ๆ ได้อีก อาทิ สื่อสังคมออนไลน์ เฟซบุ๊ก ทวิตเตอร์ เว็บไซต์ ต่างๆ เป็นต้น (Institute of Information Security, 2014 อ้างถึงใน พงศ์พนธ์ ภาวศุทธิ์, 2561)



ภาพที่ 2.3 สถิติภัยคุกคามในประเทศไทย 2563

ที่มา: ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (2563)

Abraham and Chengalur (2010) กล่าวว่า ช่องทางส่วนใหญ่ส่วนใหญ่ที่ผู้หลอกลวงนิยมใช้ในการโจมตีด้วยวิธีฟิชชิ่ง ประกอบไปด้วย อีเมล โปรแกรมแชท สื่อสังคมออนไลน์ และเว็บไซต์ ในขณะที่การโจมตีทางวิศวกรรมสังคมประเภทอื่น จะอยู่ในรูปแบบออนไลน์ ดังแสดงในภาพที่ 2.4

		Phishing	Shoulder surfing	Dumpster diving	Reverse social engineering	Waterholing	Advanced persistent threat	Baiting
Channel	E-mail	✓			✓		✓	
	Instant Messenger	✓			✓			
	Telephone, VoIP	✓			✓			
	Social Network	✓			✓			
	Cloud	✓						
	Website	✓				✓	✓	
	Physical	✓	✓	✓	✓			✓

ภาพที่ 2.4 ช่องทางที่สามารถโจมตีด้วยวิธีวิศวกรรมสังคมประเภทต่าง ๆ

ที่มา: Krombholz et al. (2015)

กรณีตัวอย่างฟิชชิ่งในประเทศไทย

จ๊ะจ๋า-พริมรตา มีข้อความไดเรกเมสเสจเข้ามาทักไอจีของจ๊ะจ๋า โดยข้อความและรูปแบบเหมือนเป็นของบริษัทไอจี โดยระบุเป็นภาษาอังกฤษประมาณว่า เรามีการทำผิดกฎของไอจี จึงต้องมีการกรอกข้อมูลยืนยันตัวบุคคลว่าเป็นเจ้าของจริง มิฉะนั้นจะถูกปิดบัญชีทันที จ๊ะจ๋าตกใจมากจึงกรอกข้อมูล พาสเวิร์ด ข้อมูลบัญชีเฟซบุ๊ก อีเมล และข้อมูลส่วนตัวไป ส่งไปในลิงก์ที่ส่งมา หลังจากนั้นสักพักบัญชีไอจีส่วนตัว @jaja_Primrata ก็เข้าไม่ได้เลย เมื่อตั้งสติได้คิดว่าโดนแฮ็กไอจี แน่เลยรีบเปลี่ยนรหัสของเฟซบุ๊ก และเมล ทำให้รอดจากการถูกแฮ็กได้ ต่อมาจ๊ะจ๋าเขียนรีพอร์ตไปชี้แจงบริษัทเฟซบุ๊กที่เป็นเจ้าของไอจี เพื่อพยายามให้บัญชีเรากลับมา พ.ต.อ.ศิริวัฒน์ เผยว่า ลักษณะที่ จ๊ะจ๋า-พริมรตา โดนแฮ็กคือการ "ฟิชชิ่ง" เป็นการสร้างลิงก์ปลอมขึ้นมา ส่วนใหญ่จะปลอมเป็นบริษัทที่น่าเชื่อถือเช่น เฟซบุ๊ก ไอจี หรืออีเมล ก่อนส่งข้อความหรือไดเรกเมสเสจไปหาบุคคลเป้าหมาย เพื่อให้เหยื่อกรอกข้อมูลส่วนตัว และรหัสล็อกอินเฟซบุ๊ก ไอจี หรืออีเมลเหยื่อ ซึ่งกรณีของ จ๊ะจ๋า-พริมรตา แฮ็กเกอร์ส่งลิงก์ฟิชชิ่งปลอม หลอกล้วงข้อมูลส่วนตัว ก่อนแฮ็กไอจีไปได้ เบื้องต้นเช็กไอพีแอดเดรสของแฮ็กเกอร์อยู่ต่างประเทศ ส่วนวัตถุประสงค์ยังไม่แน่ชัดว่าเพื่อเรียกค่าไถ หรือขโมยไอจีไปขาย เพราะคนร้ายยังไม่เผยวัตถุประสงค์ หลังจากนี้จะสืบสวนต่อไป ฝากเตือนประชาชนอย่าหลงเชื่อฟิชชิ่ง หรือกรอกข้อมูลส่วนตัว ในลิงก์ที่ไม่แน่ใจว่าเป็นของบริษัทอย่างเป็นทางการ ให้ตรวจสอบให้ถี่ถ้วน ก่อนจะใส่ข้อมูลส่วนตัวลงไป เพื่อจะได้ไม่โดนแฮ็กไอจี เฟซบุ๊ก หรือบัญชีทางโซเชียลต่าง ๆ (ไทยรัฐออนไลน์, 2563ก)

ตำรวจสืบสวน สน.ห้วยขวาง จับกุมอดีตผู้สมัคร ส.ส.พรรคภราดรภาพ “อานนท์วัฒน์ วรเมธชยางกูร” ถึงหน้าเรือนจำจังหวัดสมุทรปราการหลังสร้างเรื่องหลอกนักธุรกิจหนุ่มเป็นผู้โชคดี

ได้รับรางวัลโทรศัพท์มือถือ ออกอุบายแฮ็กข้อมูลล้วงเงินจากบัญชีไปร่วม 4 แสนบาท เผยสุดแสบจบจากประเทศเยอรมนี มีความรู้เรื่องคอม พบคดีฉ้อโกงประชาชนติดตัว 9 คดี 1 ในนั้นเอี่ยวคดีตุนขายแมสก์ของ “เสี่ยบอย-ศรสุวีร์ ภู่รวีรัศวัชรี” ขณะที่ตำรวจ สตม.จับแก๊งผิวสี ออกอุบายลวงหญิงไทย ลูกไม้เดิม ๆ พบ 1 ปีมีเงินเข้า-ออกบัญชี 280 ล้านบาท (ไทยรัฐออนไลน์, 2563ค)

ไทยเซิร์ตพบการแพร่กระจายมัลแวร์ โจมตีผู้ใช้งาน Android ในประเทศไทย โดยช่องทางการโจมตีผู้ไม่หวังดีจะส่ง SMS ที่แอบอ้างว่าเป็นการดาวน์โหลดแอปพลิเคชัน ไทยชนะ ใน SMS ดังกล่าวจะมีลิงก์ไปยังเว็บไซต์หลอกลวง เช่น หน้าเว็บไซต์ดังกล่าวสร้างเลียนแบบเว็บไซต์จริงของโครงการ ไทยชนะ โดยจะมีปุ่มที่ให้ดาวน์โหลดไฟล์ .apk มาติดตั้ง ไฟล์ดังกล่าวตรวจสอบแล้วเป็นมัลแวร์ขโมยข้อมูลทางการเงิน (บางแอนติไวรัสระบุว่าเป็นมัลแวร์สายพันธุ์ Cerberus) โดยตัวมัลแวร์ขอสิทธิ์ในการเข้าถึงข้อมูลการโทร รับส่ง SMS แอบอัดเสียง และเข้าถึงข้อมูลต่างๆ ภายในเครื่อง (ไทยเซิร์ต, 2563)

2.4 เทคนิคเหมืองข้อมูล

2.4.1 ความหมายของเหมืองข้อมูล

มีผู้ให้คำจำกัดความของเทคนิคเหมืองข้อมูล (Data Mining) ไว้หลายคำจำกัดความดังนี้

บุญเสริม กิจศิริกุล (2545, อ้างถึงใน อัณศยา เกิดคล้าย, 2553) ระบุว่า เป็นกระบวนการที่กระทำกับข้อมูลจำนวนมากเพื่อค้นหารูปแบบ และความสัมพันธ์ที่ซ่อนอยู่ในชุดข้อมูล

กนกพร ทองปลอด (2554) การสกัดหรือวิเคราะห์ ค้นหาข้อมูลที่ต้องการจากข้อมูลจำนวนมาก

ชัยชนะ กุลวรฐิต (2563) อธิบายว่า กระบวนการสกัดความรู้ที่น่าสนใจ เป็นการค้นหาความสัมพันธ์รูปแบบใหม่ซึ่งมีอยู่จริงในฐานข้อมูล แต่ได้ถูกซ่อนไว้ภายในข้อมูลจำนวนมาก ซึ่งความรู้ที่ได้จากการทำเหมืองข้อมูลนี้ จะเป็นความรู้ที่ไม่ทราบมาก่อน เพื่อนำไปใช้ในการตัดสินใจ

ด้าน Mirzakhanov (2020) ระบุว่า การทำเหมืองข้อมูลจะประกอบขึ้นจากกระบวนการทางสถิติ และการเรียนรู้ผ่านทางระบบคอมพิวเตอร์ เพื่อสร้างกฎเกณฑ์ ตัวต้นแบบในการพยากรณ์มาใช้ในการสกัดความรู้ที่น่าสนใจออกจากข้อมูลที่มีอยู่ในปริมาณที่มาก

สรุป การทำเหมืองข้อมูล เป็นกระบวนการที่มุ่งสกัด วิเคราะห์ ค้นหาความสัมพันธ์หรือรูปแบบที่อยู่ในฐานข้อมูลจำนวนมาก เพื่อนำมาประมวลผลก่อเกิดเป็นองค์ความรู้ใหม่ ๆ ที่ซ่อนอยู่ในข้อมูลที่มีอยู่แล้ว

2.4.2 วัตถุประสงค์ในการใช้เหมืองข้อมูล

วัตถุประสงค์ในการใช้เหมืองข้อมูล (Hughes, 2017) มีดังนี้

2.4.2.1 เพื่อการค้นพบองค์ความรู้ใหม่ในฐานข้อมูล (Knowledge Discovery in Databases)

2.4.2.2 เพื่อการสกัดองค์ความรู้ที่ซ่อนเร้นอยู่ (Knowledge Extraction)

2.4.2.3 เพื่อจัดการกับข้อมูลในอดีต (Data Archeology)

2.4.2.4 เพื่อสำรวจข้อมูล (Data Exploration)

2.4.2.5 เพื่อค้นหา Pattern ของข้อมูลที่ซ่อนอยู่ (Data Pattern Processing)

2.4.2.6 เพื่อใช้ขุดเจาะข้อมูล (Data Dredging)

2.4.2.7 เพื่อเก็บเกี่ยวผลประโยชน์ให้ได้มาซึ่งสารสนเทศที่มีประโยชน์

2.4.3 เทคนิคในการทำเหมืองข้อมูล

เทคนิคในการทำเหมืองข้อมูลมีหลากหลายวิธีด้วยกัน ชนวัฒน์ (2550 อ้างถึงใน ธงชัย แก้วกิริยา, 2558) กล่าวถึงเทคนิคในการทำเหมืองข้อมูลที่ได้รับความนิยมในการนำไปประยุกต์ใช้ ได้แก่ การวิเคราะห์ความสัมพันธ์ (Association) โดยมีเทคนิควิธีที่นิยมใช้เช่น เทคนิคกฎความสัมพันธ์ (Association Rules) ด้านการจัดแบ่งประเภทและการทำนาย (Classification and Prediction) เช่น เทคนิคต้นไม้ตัดสินใจ (Decision Tree) ขณะที่ Mahapatra, R. K., & Bose, I. (2001) สามารถจำแนกเทคนิคการทำเหมืองข้อมูลได้ 2 ด้าน คือด้านคณิตศาสตร์และสถิติ และด้านปัญญาประดิษฐ์

2.4.3.1 ด้านคณิตศาสตร์และสถิติ เช่น เทคนิควิธีการวิเคราะห์จำแนกกลุ่ม (Cluster Analysis) เป็นวิธีการทางสถิติที่ใช้ในการจัดกลุ่มข้อมูล พร้อมทั้งสามารถจำแนกข้อมูลใหม่ลงในกลุ่มต่าง ๆ ได้ การวิเคราะห์ความถดถอย (Regression Analysis) ซึ่งสามารถนำมาประยุกต์ใช้กับข้อมูลบางประเภท รวมถึงวิธีการทางสถิติที่ใช้แก้ปัญหาอื่น ๆ เช่น วิธีการโปรแกรมเชิงเส้น (Linear Programming)

2.4.3.2 ด้านปัญญาประดิษฐ์ เช่น เทคนิคโครงข่ายเชิงประสาท (Neural Network) การเรียนรู้โดยจดจำรูปแบบ (Pattern Recognition) จากการตรวจสอบข้อมูลในอดีต และนำรูปแบบที่ได้มาใช้พยากรณ์เพื่อสนับสนุนการตัดสินใจ โดยการสร้างทางเลือกเพื่อการตัดสินใจ (Decision Tree or Rule Induction) ถือเป็นวิธีกำหนดทางเลือกในการตัดสินใจ และค้นหาผลที่เป็นไปตามปัจจัยนั้น ๆ ชนวัฒน์ (2550 อ้างถึงใน ธงชัย แก้วกิริยา, 2558)

โดยแต่ละเทคนิคที่กล่าวข้างต้นจะเหมาะกับลักษณะของปัญหา ข้อมูล และปัจจัยที่เกี่ยวข้องที่แตกต่างกันออกไปดังแสดงในตารางที่ 2.4

ตารางที่ 2.4 เปรียบเทียบความสามารถของเทคนิคเหมืองข้อมูลกับลักษณะของข้อมูล

ลักษณะของข้อมูล	**เทคนิค**				
	Rule Induction	Decision Tree	Cluster Analysis	Neural Network	Case-Based Reasoning
รองรับข้อมูลที่หลากหลาย	ดี	ดี	ดี	ดีมาก	ดี
รองรับข้อมูลที่ไม่ถูกต้องหรือมีข้อผิดพลาด	ดี	ดี	ดี	ดี	ดี
มีความสามารถในการทำงานกับกลุ่มข้อมูลขนาดใหญ่	ดีมาก	ไม่ดี	ดีมาก	ไม่ดี	ดี
สามารถรองรับชนิดของข้อมูลได้หลายชนิด	ดี	ไม่เหมาะกับค่าต่อเนื่อง	ดีมาก	ตัวเลข 0-1 เท่านั้น	ดีมาก
ความสามารถในการพยากรณ์ได้อย่างถูกต้อง	สูง	สูง	สูง	สูงมาก	สูง
มีประสิทธิภาพในการอธิบายผลลัพธ์ที่ได้	ดีมาก	ดี	ดีมาก	ไม่ดี	ดีมาก

ตารางที่ 2.4 เปรียบเทียบความสามารถของเทคนิคเหมืองข้อมูลกับลักษณะของข้อมูล (ต่อ)

ลักษณะของข้อมูล	เทคนิค				
	Rule Induction	Decision Tree	Cluster Analysis	Neural Network	Case-Based Reasoning
นำไปใช้งานร่วมกับวิธีอื่นได้	ดี	ดี	ดี	ดี	ดี
ความสามารถในการประมวลผล	ง่าย	ง่าย	ง่าย	ยาก	ง่าย

ที่มา: Mahapatra (2001 อ้างถึงใน ธงชัย แก้วกิริยา, 2558)

จากตารางที่ 2.4 จะพบว่าในแต่ละวิธีจะมีจุดเด่น จุดด้อย รวมถึงข้อจำกัดที่แตกต่างกัน ซึ่งขึ้นอยู่กับการนำข้อมูลไปใช้งานให้เหมาะสม เช่นเทคนิคโครงข่ายประสาทเทียม (Neural Network) สามารถรองรับข้อมูลได้หลากหลาย แต่ขณะเดียวกันประสิทธิภาพในการประมวลผลจะทำได้ยาก นอกจากนี้เทคนิคต้นไม้ตัดสินใจ (Decision Tree) มีข้อดีตรงสามารถพยากรณ์ผลลัพธ์ได้แม่นยำ แต่มีข้อจำกัดในเรื่องการทำงานกับกลุ่มข้อมูลขนาดใหญ่ยังไม่ดีเท่าที่ควร

2.4.4 ขั้นตอนการทำเหมืองข้อมูล

ขั้นตอนการทำเหมืองข้อมูล (Kudyba, 2019) มีดังนี้

2.4.4.1 การกรองข้อมูล (Data Cleaning) เป็นขั้นตอนการเตรียมข้อมูลเบื้องต้นก่อนจะนำไปผ่านกระบวนการเหมืองข้อมูล จึงต้องมีการเตรียมข้อมูลก่อนดังนี้ เช่น เลือกเฉพาะคอลัมน์ที่สำคัญที่คาดว่าจะสามารถนำมาใช้ประโยชน์, แก้ไขข้อมูลให้ถูกต้องโดยกำจัดข้อมูลที่เป็นค่าว่าง รวมถึงจัดกลุ่มข้อมูลเพื่อลดการกระจายของข้อมูล

2.4.4.2 การรวมข้อมูล (Data Integration) เป็นขั้นตอนการรวมข้อมูลที่มีหลายแหล่งให้เป็นข้อมูลชุดเดียวกัน

2.4.4.3 การคัดเลือกข้อมูล (Data Selection) เป็นขั้นตอนการเลือกเฉพาะข้อมูลที่ต้องการนำมาวิเคราะห์ในการทำเหมืองข้อมูลในขั้นต่อ ๆ ไป

2.4.4.4 การแปลงรูปแบบข้อมูล (Data Transformation) เป็นการแปลงข้อมูลที่เลือกมาให้อยู่ในรูปแบบที่เหมาะสมต่อการนำไปใช้วิเคราะห์ตามอัลกอริทึมที่ใช้ในการทำเหมืองข้อมูล

2.4.4.5 การทำเหมืองข้อมูล (Data Mining) เป็นขั้นตอนการค้นหารูปแบบที่เป็นประโยชน์จากข้อมูลที่มีอยู่ โดยอาศัยหลักการทางสถิติ การรู้จำ การเรียนรู้ทางเครื่องจักร และหลักการทางคณิตศาสตร์

2.4.4.6 การแปลผลและประเมินผล (Pattern Evaluation) เป็นขั้นตอนการเลือกรูปแบบที่ยืนยันสมมติฐานที่มีเหตุผลว่ามีความเหมาะสมหรือตรงกับวัตถุประสงค์ที่ต้องการ

2.4.4.7 การนำเสนอความรู้ที่ค้นพบ (Knowledge Representation) เป็นขั้นตอนการนำเสนอความรู้ที่ค้นพบ โดยใช้เทคนิคในการนำเสนอเพื่อให้เข้าใจ

2.4.5 การวัดประสิทธิภาพของโมเดลการจำแนกประเภทข้อมูล

การประเมินประสิทธิภาพการจำแนกของโมเดล และแสดงผลด้วยเมตริกซ์เป็นส่วนสำคัญในขั้นตอนสุดท้ายของการทำเหมืองข้อมูล เนื่องจากการวัดประสิทธิภาพของการจำแนกข้อมูลจะบ่งบอกถึงความน่าเชื่อถือของโดมเดล โดยใช้รูปแบบของตาราง Confusion Matrix เป็นเครื่องมือในการคำนวณการวัดประสิทธิภาพ ดังแสดงตามตารางที่ 2.5 (กิตติพงศ์, 2555 อ้างถึงใน ธรรมสรณ์ นูมหันต์, 2558)

ตารางที่ 2.5 แสดงตาราง Confusion Matrix

	Actual Positive	**Actual Negative**
Predicted Positive	TP	FP
Predicted Negative	FN	TN

ที่มา: เอกสิทธิ์ (2557 อ้างถึงใน ธรรมสรณ์ นูมหันต์, 2558)

จากตารางที่ 2.5 ค่าที่แสดงในช่องต่าง ๆ ของตารางประกอบด้วย

True Positive (TP) คือ จำนวนข้อมูลทดสอบที่เป็นคลาส Positive และโมเดลสามารถจำแนกได้ถูกต้องว่าเป็น Positive

False Positive (FP) คือ จำนวนข้อมูลทดสอบที่ไม่ใช่คลาส Positive แต่โมเดลทำนายผิดว่าเป็นคลาส Positive

True Negative (TN) คือ จำนวนข้อมูลทดสอบที่เป็นคลาส Negative และโมเดลสามารถจำแนกได้ถูกต้องว่าเป็น Negative

False Negative (FN) คือ จำนวนข้อมูลทดสอบที่เป็นคลาส Positive และโมเดลทำนายผิดว่าเป็นคลาส Negative

โดยผลที่ได้จากตาราง Confusion Matrix ข้างต้น สามารถนำมาประเมินผลในแง่มุมต่าง ๆ ได้แก่ ค่าความถูกต้อง ค่าแม่นยำ ค่าความระลึก และประสิทธิภาพโดยรวมดังนี้

1. ค่าความถูกต้อง (Accuracy) หรืออัตราความถูกต้อง (Correctness) เป็นการแสดงถึงอัตราที่มีการทำนายที่ถูกต้องต่อจำนวนข้อมูลทั้งหมด

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}}$$

2. ค่าความแม่นยำ (Precision) เป็นการวัดความแม่นยำของโมเดล โดยพิจารณาแยกทีละคลาส

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}$$

3. ค่าเรียกคืน (Recall) เป็นการวัดความถูกต้องของโมเดล โดยพิจารณาแยกทีละคลาส

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}$$

4. ค่าความถ่วงดุล (F-Measure) เป็นการวัดค่าความแม่นยำและค่าการเรียกคืนพร้อมกันของโมเดลโดยพิจารณาแยกทีละคลาส

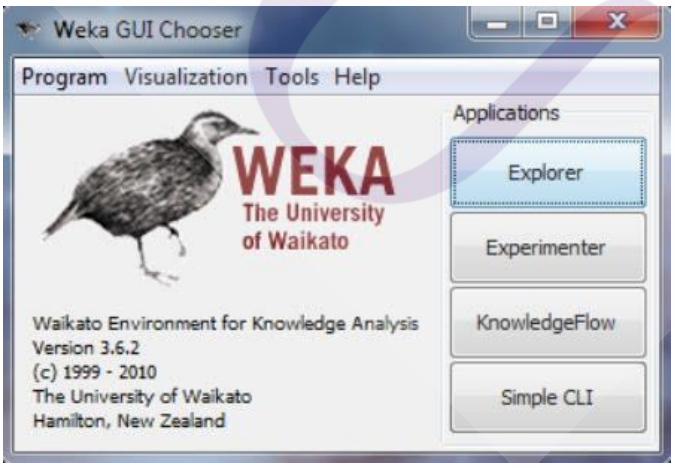
$$\text{F-Measure} = \frac{2 \times \text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}$$

2.4.6 โปรแกรมที่ใช้ทำเหมืองข้อมูล

สำหรับงานวิจัยนี้ใช้ซอฟต์แวร์เวกา (WEKA : Waikato Environment for Knowledge Analysis) ในการวิเคราะห์ความสัมพันธ์ระหว่างปัจจัยการสื่อสารและการถูกล่อลวงบนสื่อดิจิทัล เนื่องจากเป็นโปรแกรมที่มีความสามารถทางด้านเหมืองข้อมูล ได้รับความนิยมในระดับนานาชาติ

ซอฟต์แวร์เวกา เริ่มพัฒนาตั้งแต่ปี ค.ศ. 1997 โดยมหาวิทยาลัย Waikato ประเทศนิวซีแลนด์ เป็นซอฟต์แวร์ที่อยู่ใต้การควบคุม GPL License เวกาถูกพัฒนามาจากภาษาจาวาทั้งหมด โดยเน้นการทำงานด้านการเรียนรู้ด้วยเครื่อง (Machine Learning) และ การทำเหมืองข้อมูล (Data Mining)

หลักการทำงานของซอฟต์แวร์เวกา จะนำข้อมูลที่ได้จากการเก็บข้อมูลในทุก ๆ ด้านมาสร้างเป็นตัวต้นแบบของข้อมูล จากนั้นจะทำการวิเคราะห์หาค่าต่าง ๆ โดยสามารถทำการเลือกรูปแบบการวิเคราะห์ได้หลากหลาย เพื่อให้ได้ผลลัพธ์ของข้อมูลที่ต้องการ



ภาพที่ 2.5 โปรแกรม Weka

2.4.7 ประโยชน์ของเหมืองข้อมูล

2.4.7.1 ช่วยชี้แนวทางการตัดสินใจและคาดการณ์ผลลัพธ์ที่จะได้จากการตัดสินใจ

2.4.7.2 เพิ่มความเร็วในการวิเคราะห์ฐานข้อมูลขนาดใหญ่

2.4.7.3 ค้นหาส่วนประกอบที่ซ่อนอยู่ภายในเอกสาร รวมถึงความสัมพันธ์ของส่วนประกอบต่าง ๆ ด้วย

2.4.7.4 เชื่อมโยงหน่วยงานต่าง ๆ ภายในองค์กร

2.4.7.5 การจัดกลุ่มข้อมูล เช่น จัดกลุ่มลูกค้าทั้งหมดของบริษัทประกันภัยที่ประสบอุบัติเหตุ ลักษณะเดียวกันเพื่อดำเนินการต่าง ๆ ตามนโยบายของบริษัท

2.5 ต้นไม้ตัดสินใจ

2.5.1 ความหมายของต้นไม้ตัดสินใจ

พยูน (2548 อ้างถึงใน ธงชัย แก้วกิริยา, 2558) อธิบายว่า เป็นแบบจำลองทางคณิตศาสตร์เพื่อหาทางเลือกที่ดีที่สุด โดยการนำข้อมูลมาสร้างแบบจำลองการพยากรณ์ในรูปแบบของโครงสร้างต้นไม้ ซึ่งมีการเรียนรู้ข้อมูลแบบมีผู้สอน (Supervised Learning) สามารถสร้างแบบจำลองการจัดหมวดหมู่ (Clustering) ซึ่งได้จากกลุ่มของข้อมูลที่กำหนดไว้ล่วงหน้า (Training Set) ได้โดยอัตโนมัติ และสามารถพยากรณ์กลุ่มของรายการที่ยังไม่เคยนำมาจัดหมวดหมู่ได้

โดยมีกฎในรูปแบบ “ถ้าเงื่อนไขแล้วผลลัพธ์” เช่น

“If Income = High and Married = No THEN Risk = Poor”

“If Income = High and Married = Yes THEN Risk = Good”

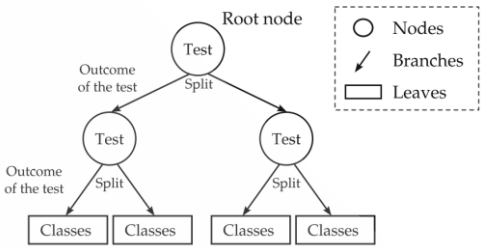
2.5.2 ส่วนประกอบของต้นไม้ตัดสินใจ

ส่วนประกอบของต้นไม้ตัดสินใจ ประกอบไปด้วย 3 องค์ประกอบหลักดังนี้

2.5.2.1 โหนด (Node) คือ คุณสมบัติต่าง ๆ เป็นจุดแยกข้อมูลว่าจะให้ไปในทิศทางใด ซึ่งโหนดที่อยู่สูงกว่าเรียกหว่า โหนดราก (Root Node)

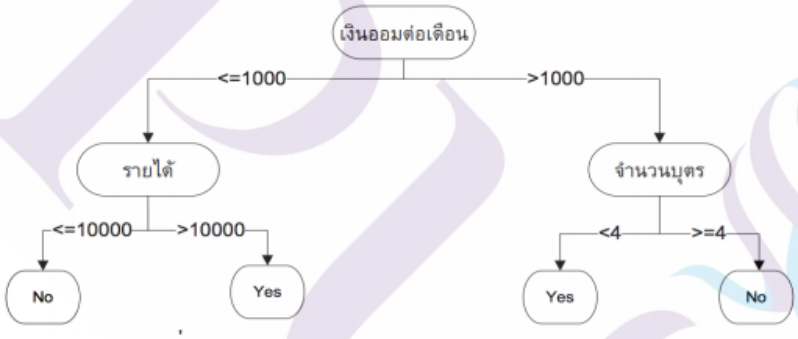
2.5.2.2 กิ่ง (Branch) คือ คุณสมบัติของคุณสมบัติในโหนดที่แตกออกมาโดยจำนวนของกิ่งจะเท่ากับคุณสมบัติของโหนด

2.5.2.3 ใบ (Leaf) คือ กลุ่มของผลลัพธ์ในการแยกแยะข้อมูล โดยสามารถแสดงตัวอย่างต้นไม้ตัดสินใจได้ดังภาพที่ 2.6



ภาพที่ 2.6 ส่วนประกอบของต้นไม้ตัดสินใจ

ที่มา: Kozak, J. (2018)



ภาพที่ 2.7 ตัวอย่างต้นไม้ตัดสินใจ

ที่มา: ศุภชัย ประคองศิลป์ (2551)

2.5.3 การสร้างต้นไม้ตัดสินใจ

หลักพื้นฐานของการสร้างต้นไม้ตัดสินใจ (Decision Tree) เป็นการสร้างในลักษณะบนลงล่าง (Top-Down) คือ เริ่มจากการสร้างรากของต้นไม้ แล้วจึงค่อยแตกกิ่งไปจนถึงใบ โดยสามารถแสดงขั้นตอนการสร้างต้นไม้ตัดสินใจได้ดังนี้ (Han and Kamber, 2011)

2.5.3.1 จุดเริ่มต้นของต้นไม้ จะมีเพียงโหนดเดียวที่แสดงถึงชุดข้อมูลฝึก (Training Set)

2.5.3.2 ถ้าข้อมูลทั้งหมดอยู่ในกลุ่มเดียวกันแล้ว ให้โหนดนั้นเป็นใบ และตั้งชื่อแยกตามกลุ่มของข้อมูลนั้น

2.5.3.3 ถ้าในโหนดมีข้อมูลหลายกลุ่มปะปนอยู่ จะต้องวัดผ่านค่าเกน (Gain) ของแต่ละแอตทริบิวต์ของข้อมูล เพื่อใช้เป็นเกณฑ์ในการคัดเลือกแอตทริบิวต์ที่มีความสามารถในการแบ่งแยกข้อมูลออกเป็นกลุ่มต่าง ๆ ได้ดีที่สุด โดยแอตทริบิวต์ที่มีค่าเกน (Gain) มากที่สุดจะถูกเลือกให้เป็นตัวทดสอบหรือเป็นแอตทริบิวต์ ที่ใช้ในการตัดสินใจโดยแสดงในรูปของโหนดต้นไม้

2.5.3.4 กิ่งของต้นไม้ถูกสร้างขึ้นจากค่าต่าง ๆ ที่เป็นไปได้ของโหนดทดสอบ และข้อมูลจะถูกแบ่งออกตามกิ่งต่าง ๆ ที่สร้างขึ้น

2.5.3.5 ทำการวนซ้ำเพื่อหาแอตทริบิวต์ที่มีค่าเกน (Gain) มากที่สุด สำหรับข้อมูลที่ถูกแบ่งแยกออกมาในแต่ละกิ่งเพื่อนำแอตทริบิวต์ มาสร้างเป็นโหนดตัดสินใจต่อไป โดยแอตทริบิวต์ที่ถูกเลือกมาเป็นโหนดแล้วจะไม่ถูกเลือกมาอีกสำหรับโหนดต่อ ๆ ไป

2.5.3.6 ทำการวนซ้ำ เพื่อแบ่งข้อมูลและแตกกิ่งของต้นไม้ไปเรื่อย ๆ โดยการวนซ้ำจะสิ้นสุดต่อเมื่อเงื่อนไขข้อใดข้อหนึ่งต่อไปนี้เป็นจริง

2.5.4 การคำนวณค่า Information Gain

ค่า Information Gain เป็นโครงสร้างที่ใช้แสดงกฎที่ได้จากเทคนิคการจำแนกประเภทข้อมูล โดยต้นไม้ตัดสินใจจะมีลักษณะคล้ายโครงสร้างของต้นไม้ที่จะมีโหนดแสดงแอตทริบิวต์สำหรับการสร้างต้นไม้ตัดสินใจแต่ละครั้ง มีประเด็นสำคัญที่จะต้องพิจารณาคือ จะเลือกแอตทริบิวต์ใดมาทำหน้าที่เป็นโหนดราก (Root Node) ซึ่งกระบวนการในการสร้างต้นไม้ รวมถึงสร้างต้นไม้ย่อย จะมีเงื่อนไขที่ใช้ในการพิจารณาคือการคำนวณค่ามาตรฐานแกน (Gain Criterion) ซึ่งเป็นค่าที่จะบ่งบอกว่าแอตทริบิวต์นั้น สามารถจำแนกกลุ่มของข้อมูลได้ดีเพียงใด โดยที่ค่า Information Gain สามารถคำนวณได้ดังสมการต่อไปนี้

$$I(S_1,S_1,...,S_n) = - \sum_{i=0}^{n} \frac{S_1}{s} \log_2 \frac{S_1}{s}$$

เมื่อ S แทน เซตของข้อมูลโดยประกอบด้วยข้อมูล s เรคคอร์ด

n แทน จำนวนกลุ่มทั้งหมดที่ต่างกันของข้อมูลชุดนั้น

C_i แทน กลุ่มในลำดับที่ i โดยที่ i มีค่าระหว่าง 1 ถึง n

S_i แทน จำนวนข้อมูลที่เป็นสมาชิกของ s และอยู่ในกลุ่ม C_i

S_{ij} แทน จำนวนข้อมูลที่เป็นสมาชิกของ s ในกลุ่ม C_i จากการแบ่งข้อมูลด้วยค่าที่เป็นไปได้ของแอททริบิวต์ A

j แทน ค่าระหว่าง 1 ถึง v

ค่าเอ็นโทรปีของแอททริบิวต์ A ซึ่งมีค่าแอดทริบิวต์เป็น $(a1, a2, a3,..., av)$ หาได้จากการแสดงดังสมการต่อไปนี้

$$E(A) = \sum_{j=1}^{v} \frac{s_{1j} + \ldots + s_{nj}}{s} l(s_{1j}, s_{2j}, \ldots, s_{nj})$$

ดังนั้นจะสามารถพิจารณาค่ามาตรฐานเกน (Gain) ได้แสดงดังสมการต่อไปนี้

$$Gain(A) = I(S_1, S_2, \ldots, S_n) - E(A)$$

2.5.5 การทำเหมืองข้อมูลโดยใช้เทคนิคต้นไม้ตัดสินใจ ID3

ขั้นตอนการสร้างต้นไม้ตัดสินใจด้วยวิธี ID3 นั้นจะสร้างต้นไม้ตัดสินใจจากบนลงล่างด้วยการตัดสินใจว่าคุณลักษณะใดควรที่จะเป็นรากของต้นไม้ด้วยค่า Information Gain (Hamid, 2009) และค่า Entropy (Volkenstein, 2009) ยกตัวอย่างในการสร้างต้นไม้ตัดสินใจในการที่จะไปเล่นกอล์ฟหรือไม่เล่นกอล์ฟ โดยดูได้จากตัวแปรด้านภูมิอากาศ จากตารางดังต่อไปนี้

ตารางที่ 2.6 ข้อมูลของตัวแปรที่ใช้ในการตัดสินใจในการไปเล่นกอล์ฟ

Outlook	Temp	Humidity	Windy	Play Golf
Rainy	Hot	High	False	No
Rainy	Hot	High	True	No
Overcast	Hot	High	False	Yes
Sunny	Mild	High	False	Yes
Sunny	Cool	Normal	False	Ys
Sunny	Cool	Normal	True	No
Overcast	Cool	Normal	True	Yes
Rainy	Mild	High	False	No
Rainy	Cool	Normal	False	Yes
Sunny	Mild	Normal	False	Yes
Rainy	Mild	Normal	True	Yes
Overcast	Mild	High	True	Yes
Overcast	Hot	Normal	False	Yes
Sunny	Mild	High	True	No

ที่มา: Pimporn (2019)

หลังจากนั้นนำค่าตัวแปรที่ได้มาคำนวณค่า Entropy ของเซตของข้อมูลหรือ E(S) ซึ่งสามารถคำนวณได้จากสมการดังต่อไปนี้

$$E(S) = \sum_{i=1}^{c} -p_i \log_2 p_i$$

ซึ่งชุดข้อมูลของ S ประกอบด้วย {s1, s2, …, sn} และความน่าจะเป็นที่จะเกิดเหตุการณ์ si มีค่าเท่ากับ pi จากข้อมูลของตัวอย่างดังรูป จะเห็นได้ว่า จำนวนของเหตุการณ์ทั้งหมดเท่ากับ 14 เหตุการณ์ โดยผลลัพธ์คือ เล่นกอล์ฟหรือ Yes จำนวนการเกิดเหตุการณ์ทั้งหมดเท่ากับ 9 ครั้ง และไม่เล่นกอล์ฟหรือ No จำนวนการเกิดเหตุการณ์ทั้งหมดเท่ากับ 5 ครั้ง ดังนั้นจะคำนวณค่า Entropy เท่ากับ E(S) = Entropy(5,9) = - (0.36log20.36) - (0.64log20.64) = 0.94 สำหรับตัวอย่างการคำนวณการสร้างต้นไม้ตัดสินใจเพื่อเริ่มสร้างรากของต้นไม้โดยพิจารณาจากคุณลักษณะของ outlook สามารถคำนวณค่า Entropy เท่ากับ E(PlayGolf , Outlook) = P(Sunny) × E(3,2) + P(Overcast) × E(4,0) + P(Rainy) × E(2,3) = 0.693 สำหรับค่า Information Gain หาได้จากสมการดังต่อไปนี้

$$\mathrm{Gain(S,A)} = \mathrm{E(S)\text{-}E(S,A)}$$

ดังนั้น ค่า Information Gain ของคุณลักษณะ Outlook เท่ากับ 0.94-0.693 = 0.247 แสดงดังตารางที่ 2.7

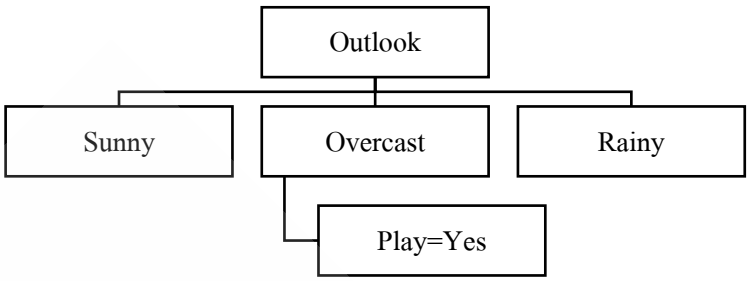
ตารางที่ 2.7 ค่า Information Gain ของแต่ละคุณลักษณะ

		Play Golf	
		Yes	**No**
Outlook	**Sunny**	3	2
	Overcast	4	0
	Rainy	2	3
Information Gain = 0.247			

		Play Golf	
		Yes	**No**
Temp	**Hot**	2	2
	Mild	4	2
	Cool	3	1
Information Gain = 0.029			

		Play Golf	
		Yes	**No**
Humidity	**High**	3	4
	Normal	6	1
Information Gain = 0.152			

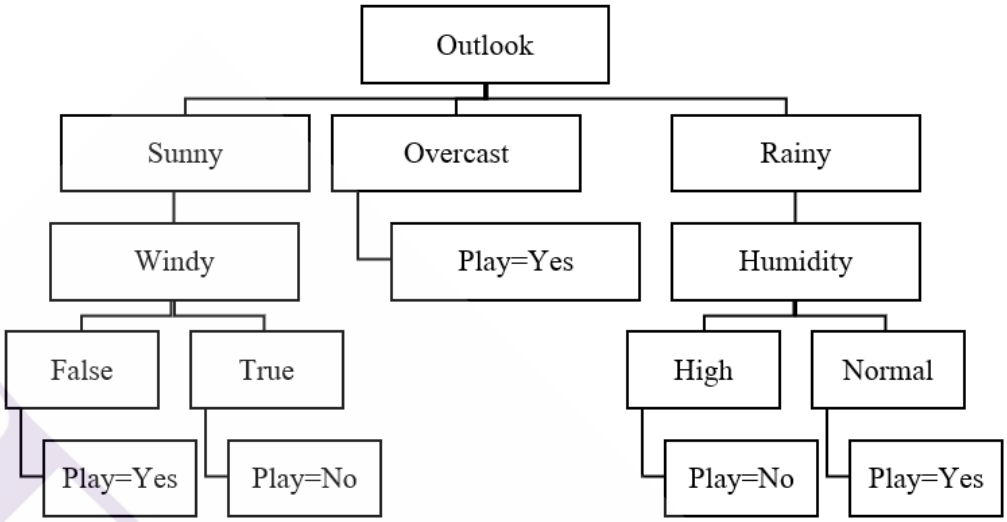
		Play Golf	
		Yes	**No**
Windy	**False**	6	2
	True	3	3
Information Gain = 0.048			



ภาพที่ 2.8 แผนภูมิแสดงคุณลักษณะในการตัดสินใจสำหรับการเลือกเป็นโหนดราก

ที่มา: Pimporn (2019)

โดยตารางที่ 2.7 ค่า Information Gain ของแต่ละคุณลักษณะ การเลือกคุณลักษณะที่ใช้สำหรับเป็นโหนดรากจะเลือกจากค่า Information Gain ที่มากที่สุด จากตารางที่ 2.7 ค่า Information Gain ของแต่ละคุณลักษณะ จะเห็นได้ว่า ค่า information Gain สูงสุด คือ คุณลักษณะ outlook ดังนั้นจึงถูกเลือกเป็นคุณลักษณะในการตัดสินใจสำหรับการเลือกเป็นโหนดรากแสดงดังภาพที่ 2.8 แผนภูมิแสดงคุณลักษณะในการตัดสินใจสำหรับการเลือกเป็นโหนดราก โดยคุณลักษณะ Overcast มีค่า Entropy เท่ากับ 0 คือเป็นการตัดสินใจเพียงในทิศทางเดียวหรือความเป็นไปได้ที่จะเล่นกอล์ฟทั้งหมด (Kotu, V., & Deshpande, 2014) สำหรับคุณลักษณะอื่น ๆ ที่มีค่า Entropy ไม่เท่ากับศูนย์จะถูกคำนวณค่า information Gain และเลือกค่าที่มากที่สุดเพื่อกำหนดเป็นโหนดรากต่อ ๆ มา และจนกระทั่งมีค่า Entropy เท่ากับศูนย์โดยข้อมูลทั้งหมดถูกจำแนกกลุ่มและสามารถสร้างต้นไม้ตัดสินใจได้ดังภาพที่ 2.9 แผนภูมิแสดงข้อมูลทั้งหมดถูกจำแนกกลุ่มและสร้างต้นไม้ตัดสินใจ



ภาพที่ 2.9 แผนภูมิแสดงข้อมูลทั้งหมดถูกจำแนกกลุ่มและสร้างต้นไม้ตัดสินใจ

ที่มา: Pimporn (2019)

2.6 นาอีฟเบย์

2.6.1 ความหมายของนาอีฟเบย์

ภัทราพร ช่างจูม (2554) เป็นโมเดลการจำแนกกลุ่มที่ใช้หลักความน่าจะเป็นอยู่บนพื้นฐานของ Bayes' Theorem

ธนกร เจริญเชาว์ (2554) เป็นการคำนวณหาความน่าจะเป็นของแต่ละกลุ่มข้อมูล หรือคลาส (Class) ซึ่งเมื่อกำหนดลักษณะประจำ (Attribute) และค่าลักษณะประจำแต่ละตัวจะใช้ในการทำนาย ซึ่งการคำนวณหาค่าความน่าจะเป็นของทุกคลาสและเปรียบเทียบกัน ค่าความน่าจะเป็นที่สูงที่สุดของคลาสใด ๆ จะเป็นผลของการทำนายเพียงค่าเดียว โดยถือว่าลักษณะประจำ แต่ละตัวมีความเป็นอิสระต่อกัน (Class Conditional Independence)

ดังนั้นเทคนิคของนาอีฟเบย์ คือ การสร้างโมเดลโดยการคำนวณหาค่าความน่าจะเป็นของแต่ละกลุ่มข้อมูล ทำการเปรียบเทียบกัน เพื่อหาคลาสที่มีค่าความน่าจะเป็นสูงที่สุด โดยที่ข้อมูลแต่ละตัวมีความเป็นอิสระแยกออกจากกัน

2.6.2 การทำนายเหตุการณ์ด้วยเทคนิคนาอีฟเบย์

กำหนดให้ P (H) ความน่าจะเป็นที่จะเกิดเหตุการณ์ H และ P (H|E) คือความน่าจะเป็นที่จะเกิดเหตุการณ์ H เมื่อเกิดเหตุการณ์ E จากตัวแปรที่กำหนดและแนวคิดของ Bayes' Theorem นั้นสามารถแสดงได้ดังสมการต่อไปนี้

$$P(H|E) = \frac{[P\ (E|H)\ \times\ P(H)]}{P(E)}$$

เช่น การทำนายว่าฝนจะตกเมื่อมีเหตุการณ์มีเมฆดำ

กำหนดให้ H คือ เหตุการณ์ที่ฝนตก

E คือ เหตุการณ์ที่มีเมฆดำและสามารถทำนายสภาพจราจร

$$P(\text{ฝนตก} \mid \text{เมฆดำ}) = \frac{[P\ (\text{เมฆดำ} \mid \text{ฝนตก})\ \times\ P\ (\text{ฝนตก})]}{P\ (\text{เมฆดำ})}$$

กำหนดให้ P (เมฆดำ | ฝนตก) คือ ความน่าจะเป็นที่มีเมฆดำเมื่อฝนตก ซึ่งจะพิจารณาการเกิดเมฆดำเมื่อมีเหตุการณ์ฝนตกเท่านั้น ความน่าจะเป็นนี้สามารถเก็บรวบรวมโดยใช้หลักการทางสถิติ

P (ฝนตก) คือ ความน่าจะเป็นที่ฝนตก

P (เมฆดำ) คือ ความน่าจะเป็นที่มีเมฆดำ

การคำนวณการจำแนกกลุ่มของเหตุการณ์ที่มีการเกิดของเหตุการณ์ต่าง ๆ ที่ใช้ในการจำแนกกลุ่มมากกว่า 1 ชนิด สามารถแสดงได้ดังสมการต่อไปนี้

$$P\ H|E1, E2, \ldots, En\ = \frac{[P\ E1, E2, \ldots, En|H\ \times\ P(H)]}{P(E1, E2, \ldots, En)}$$

เมื่อกำหนดให้เหตุการณ์ $E1, E2, \ldots, En$ คือ เหตุการณ์ n เหตุการณ์ที่ใช้ในการจำแนกกลุ่ม และแต่ละเหตุการณ์ต่าง ๆ ที่ใช้ในการจำแนกกลุ่มอิสระต่อกัน

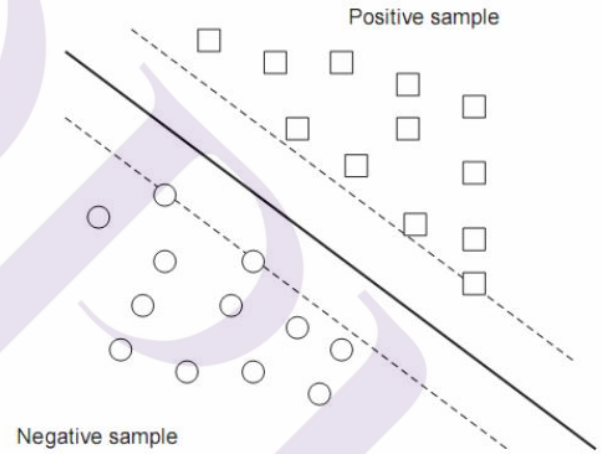
2.7 ซัพพอร์ตเวกเตอร์แมชชีน

2.7.1 ความหมายของซัพพอร์ตเวกเตอร์แมชชีน

จิรา แก้วสุวรรณ์ (2549) เป็นเทคนิคที่ใช้ในการแก้ปัญหาทางด้านการรู้จำรูปแบบข้อมูล โดยอาศัยหลักสัมประสิทธิ์ของสมการเพื่อสร้างเส้นแบ่งแยกกลุ่มข้อมูลที่ถูกป้อนเข้าสู่กระบวนการสอนให้ระบบเรียนรู้ โดยเน้นไปยังเส้นแบ่งแยกของกลุ่มข้อมูลได้ดีที่สุด (Optimal Separating Hyperplane)

พีรญา ดุนขุนทด (2553) ได้ให้ความความหมายว่า เป็นโครงข่ายประสาทเทียมรูปแบบใหม่ใช้สำหรับแก้ไขข้อบกพร่องต่าง ๆ ของโครงข่ายประสาทเทียมแบบดั้งเดิม โดยอาศัยพื้นฐานความรู้มาจากเรื่องทฤษฎีการเรียนรู้ทางสถิติ

พรพล ธรรมรงค์รัตน์ (2552) เป็นแนวคิดที่ใช้เพื่อหาระนาบการตัดสินใจในการแบ่งข้อมูลออกเป็นสองส่วน ใช้สำหรับข้อมูลที่มีมิติของข้อมูลสูง แสดงดังภาพที่ 2.10



ภาพที่ 2.10 ภาพประกอบระนาบตัดสินใจของ SVM

ที่มา: พรพล ธรรมรงค์รัตน์ (2552)

กำหนดให้ $x_i, y_i, \ldots, x_n, y_n$ เป็นตัวอย่างที่ใช้สำหรับการสอน

โดยที่ n คือ จำนวนข้อมูลตัวอย่าง

m คือ จำนวนมิติข้อมูลเข้า

y คือ ผลลัพธ์ มีค่า +1 หรือ -1

สามารถแสดงได้ดังสมการต่อไปนี้

$$x_i, y_i \ , \ldots , \ x_n, y_n \quad \text{เมื่อ } x \in R^m, y \in \{+1, -1\}$$

สำหรับปัญหาเชิงเส้น มิติข้อมูลขนาดสูงได้ถูกแบ่งเป็น 2 กลุ่ม โดยระนาบตัดสินใจซึ่งคำนวณได้ดังสมการต่อไปนี้

$$w \cdot x \ + b = 0$$

เมื่อ w คือ ค่าน้ำหนัก และ b คือค่า bias ซึ่งใช้สำหรับจำแนกประเภทของข้อมูลดังสมการต่อไปนี้

$$w \cdot x \ + b > 0 \text{ ถ้า } y_i - +1 \text{ และ } \ w \cdot x \ + b < 0 \text{ ถ้า } y_i - -1$$

2.7.2 การทำนายเหตุการณ์ด้วยเทคนิคซัพพอร์ตเวกเตอร์แมชชีน

ยกตัวอย่างการนำซัพพอร์ตเวกเตอร์แมชชีนมาใช้สำหรับการทำนายโอกาสการเป็นมะเร็งของคนเพื่อวิเคราะห์กำหนดเบี้ยทำประกันชีวิต โดยกำหนดข้อมูลผู้ที่เคยป่วยเป็นมะเร็งจำนวน 1,000 คน เข้าสู่กระบวนการทำนาย ดังแสดงผลที่ตาราง 2.8

ตารางที่ 2.8 ข้อมูลผู้ที่เคยป่วยเป็นมะเร็งจำนวน 1,000 คน

คนที่	เพศ	อายุ	จำนวนพี่น้องป่วยเป็นมะเร็ง	น้ำหนัก	รายได้ต่อปี
1	ชาย	50	มี	40	100,000
2	หญิง	30	ไม่มี	60	50,000
…	…	…	…	…	…
1,000	ชาย	35	มี	55	200,000

ที่มา: จินตนา โนนวงศ์ (2558)

หลังจากนั้นนำข้อมูลผู้ที่ยังไม่ป่วยเป็นมะเร็งมาทดสอบเพื่อทำนายจัดกลุ่ม ว่าข้อมูลดังกล่าวจะอยู่ในกลุ่มของคนที่เป็นมะเร็ง หรือกลุ่มคนที่ไม่เป็นมะเร็ง เช่น นาย ก ซึ่งในตอนนี้ยังไม่ได้ป่วยเป็นมะเร็ง ซึ่งมีข้อมูลแสดงดังตารางที่ 2.9 ผลในการทำนายนั้นอาจจะจัดให้ นาย ก อยู่ในกลุ่มคนที่เป็นมะเร็ง หรือ กลุ่มคนที่ไม่เป็นมะเร็งก็ได้ จากนั้นบริษัทก็จะนำข้อมูลดังกล่าวไปวางแผนในการเก็บค่าเบี้ยประกันต่อไป

ตารางที่ 2.9 ผลการจำแนกข้อมูล

คนที่	เพศ	อายุ	จำนวนพี่น้องป่วยเป็นมะเร็ง	น้ำหนัก	รายได้ต่อปี
1	ชาย	50	มี	40	100,000

ที่มา: จินตนา โนนวงศ์ (2558)

จุดเด่นของซัพพอร์ตเวกเตอร์แมชชีน คือด้านประสิทธิภาพในการทดสอบ จำแนกกลุ่มข้อมูลที่ไม่เคยพบเห็นมาก่อน แล้วมีความถูกต้องอยู่ในระดับที่สูง

2.8 งานวิจัยที่เกี่ยวข้อง

พงศ์พนธ์ ภาวศุทธิ์ (2561) ได้ศึกษาสาเหตุเชิงลึกของการโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยมีวัตถุประสงค์เพื่อศึกษาถึงสาเหตุเชิงลบึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล ว่ามีสาเหตุใดบ้างที่ส่งผลให้บุคคลที่ได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ เช่น อีเมล เว็บไซต์ สื่อสังคมออนไลน์ เป็นต้น นั้นตัดสินใจกระทำตามสิ่งที่ผู้โจมตีต้องการและถูกโจมตีโดยงานวิจัยนี้เป็นการศึกษาวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งเก็บข้อมูลด้วยการสัมภาษณ์เชิงลึก (In-Depth Interview) จากผู้ให้สัมภาษณ์ทั้งสิ้น 18 ท่าน ที่เคยมีประสบการณ์ได้รับสารสนเทศที่เป็นภัยคุกคามโดยมีเหตุการณ์ที่หลากหลายและแตกต่างกัน โดยคำถามที่ใช้ในการสัมภาษณ์เป็นคำถามแบบปลายเปิด เพื่อให้ผู้สัมภาษณ์สามารถให้ข้อมูลเพิ่มเติมได้ ผลการวิจัยพบว่า

สาเหตุที่ส่งผลต่อการถูกโจมตีด้วยวิธีวิศวกรรมสังคมนั้นสามารถแบ่งได้เป็น 2 กรณี คือ กรณีที่หนึ่งเป็นบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมและถูกโจมตี จะมีปัจจัยที่ส่งผล ได้แก่ การตัดสินใจอย่างไม่มีเหตุผลที่เกิดขึ้นจาก ความอยากรู้อยากเห็น ความกลัว และความโลภ ซึ่งเป็นอารมณ์ความรู้สึกพื้นฐานของมนุษย์ โดยผู้โจมตีจะใช้ลักษณะเฉพาะของสารสนเทศ เช่น ช่องทาง เนื้อหา รูปแบบ และรูปภาพ ที่สร้างมาเพื่อให้ผู้ถูกโจมตีนั้นเกิดอารมณ์ความรู้สึกอย่างใดอย่างหนึ่งข้างต้นและตัดสินใจอย่างไม่มีเหตุผลจนส่งผลให้ถูกโจมตีได้ ส่วนกรณีที่สองเป็นบุคคลที่เคยได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมในรูปแบบต่าง ๆ แต่ไม่ถูกโจมตี จะมีปัจจัยที่ส่งผลได้แก่ การรับรู้ภัยคุกคาม ซึ่งเกิดขึ้นจากประสบการณ์ก่อนหน้า และการแจ้งเตือน โดยเมื่อบุคคลมีการรับรู้ภัยคุกคามมากเพียงพอแล้วจะมีการตัดสินใจที่ใช้เหตุผลไตร่ตรองมากยิ่งขึ้นและไม่ถูกโจมตี ข้อจำกัดของงานวิจัยนี้คือการที่อัตราส่วนผู้ให้สัมภาษณ์ของเพศหญิงมีมากกว่าเพศชายโดยเป็นเพศหญิง 14 ท่าน และเพศชาย 4 ท่าน และผลของการวิจัยของผู้ให้สัมภาษณ์เพศชายที่พบว่าเหตุการณ์ส่วนใหญ่จะเป็นการได้รับสารสนเทศที่เป็นภัยคุกคามด้วยวิธีการทางวิศวกรรมสังคมแต่ไม่ถูกโจมตี ดังนั้นการนำผลการวิจัยนี้ไปใช้อาจต้องคำนึงถึงเรื่องเพศด้วยเช่นกัน ในส่วนของข้อแนะนำสำหรับงานวิจัยต่อเนื่องนั้น เนื่องจากสาเหตุของการถูกโจมตีด้วยวิธีวิศวกรรมสังคมสะท้อนให้เห็นว่า อารมณ์และความรู้สึกต่าง ๆ ส่งผลให้ผู้ถูกโจมตีตัดสินใจอย่างไม่มีเหตุผล และถูกโจมตีในที่สุด แต่การรับรู้ภัยคุกคามที่สูงนั้นจะสามารถยับยั้งการถูกโจมตีได้ จึงควรศึกษาหาแนวทาง การป้องกันการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม โดยอาจศึกษาลึกลงไปในสาเหตุต่าง ๆ ว่าควรจะสร้างการรับรู้ภัยคุกคามและป้องกันอย่างไรให้ได้ประสิทธิภาพสูงที่สุด

อลิษา สายแผ้ว (2556) ได้ศึกษาประสิทธิภาพของกฎหมายไทยในการรับมือกับอาชญากรรมข้ามชาติในรูปแบบฟิชชิ่ง (Phishing) ศึกษาเฉพาะกรณีกระทำต่อระบบธนาคารทางอินเทอร์เน็ต (Internet Banking) โดยมีวัตถุประสงค์เพื่อศึกษาสภาพปัญหาและต้นทุนของการกระทำความผิดในรูปแบบฟิชชิ่งตลอดจนพิจารณาความเหมาะสมในการกำหนดโทษทางอาญาและศึกษาระบบยุติธรรมทางเลือก เพื่อหาแนวทางในการยับยั้งการกระทำนั้นอย่างมีประสิทธิภาพ วิธีการศึกษาจะทำการศึกษาทั้งในเชิงนิติศาสตร์และเศรษฐศาสตร์ ในเชิงนิติศาสตร์จะทำการศึกษากฎหมายไทยเปรียบเทียบกับกฎหมายอังกฤษ เพื่อพิจารณาว่ากฎหมายไทยมีประสิทธิภาพเพียงพอ

ในการรับมือกับอาชญากรรมข้ามชาติในรูปแบบฟิชชิ่งที่กระทำต่อระบบธนาคารทางอินเทอร์เน็ตหรือไม่ ในเชิงเศรษฐศาสตร์จะทำการศึกษาแนวคิดเชิงพฤติกรรม และเศรษฐศาสตร์อาชญากรรมโดยมุ่งอธิบายพฤติกรรมของอาชญากร ผ่านโครงสร้างผลประโยชน์และต้นทุน ผลการวิจัยพบว่าผู้ที่สามารถหลีกเลี่ยงข้อพิพาทได้ดีที่สุด โดยมีต้นทุนต่ำที่สุดควรเป็นผู้รับผิดชอบในการแก้ปัญหาที่เกิดขึ้นเป็นหลัก อันได้แก่ ผู้ใช้บริการธนาคารทางอินเทอร์เน็ตเอง แต่การป้องปรามจะมีประสิทธิภาพก็ต่อเมื่อ ผู้ที่มีแนวโน้มจะกระทำผิด เห็นว่ากระบวนการยุติธรรมทางอาญาสร้างต้นทุน หรือลดแรงจูงใจ ได้เท่ากับผลประโยชน์ที่จะได้รับจากการทำฟิชชิ่งสำเร็จ หรือความเสียหายที่ฟิชเชอร์เป็นผู้ก่อแก่สังคม ดังนั้นการป้องปรามจึงมิอาจผลักดันภาระให้แก่ผู้ใช้บริการได้ทั้งหมด แต่ต้องมีโครงสร้างแรงจูงใจให้อยู่ในระดับที่เหมาะสมสำหรับทุก ๆ ฝ่ายที่เกี่ยวข้องอีกประการหนึ่ง ซึ่งต้องอาศัยทั้งมาตรการทางกฎหมายและมาตรการทางด้านอื่น ๆ ควบคู่กันไป

ศุภกร จูฑะพล (2557) ได้ศึกษาทัศนคติ พฤติกรรม และความคล่องดิจิทัลของกลุ่มดิจิทัลเนทีฟ โดยมีวัตถุประสงค์เพื่อศึกษาทัศนคติต่อการดำเนินชีวิต พฤติกรรมการดำเนินชีวิต และความคล่องดิจิทัลของกลุ่มดิจิทัลเนทีฟ เพื่อศึกษาความสัมพันธ์ของทัศนคติต่อการดำเนินชีวิต และพฤติกรรมการดำเนินชีวิตที่มีต่อความคล่องดิจิทัลของกลุ่มดิจิทัลเนทีฟ และเพื่อศึกษาตัวแปรที่เป็นปัจจัยพยากรณ์ความคล่องดิจิทัล งานวิจัยนี้ เป็นการศึกษาวิจัยเชิงปริมาณ โดยการใช้แบบสอบถามเป็นเครื่องมือในการเก็บข้อมูลกับกลุ่มตัวอย่างดิจิทัลเนทีฟผู้มีอายุ 15-24 ปี และมีประสบการณ์ในการใช้งานอินเทอร์เน็ตไม่ต่ำกว่า 5 ปี ในเขตกรุงเทพมหานคร จำนวน 402 คน ผลการวิจัยพบว่า มีกลุ่มทัศนคติต่อการดำเนินชีวิตทั้งหมด 7 กลุ่ม กลุ่มพฤติกรรมการดำเนินชีวิตทั้งหมด 5 กลุ่ม และกลุ่มคุณลักษณะดิจิทัลเนทีฟทั้งหมด 3 กลุ่ม โดยกลุ่มทัศนคติและพฤติกรรมการดำเนินชีวิตของดิจิทัลเนทีฟทุกกลุ่ม มีความสัมพันธ์กับความคล่องดิจิทัลอย่างมีนัยยะสำคัญทางสถิติ ทั้งนี้ กลุ่มคุณลักษณะดิจิทัลเนทีฟที่ชื่อว่ากลุ่ม The Digital Passenger เป็นตัวแปรที่เป็นปัจจัยพยากรณ์ความคล่องดิจิทัล

กันต์นลิน เปรมใจสุข (2558) ได้ศึกษาอิทธิพลของปัจจัยการสื่อสารแบบบอกต่อที่มีผลต่อพฤติกรรมผู้บริโภคในธุรกิจอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อศึกษาอิทธิพลของปัจจัยการสื่อสารแบบบอกต่อผ่านสื่ออิเล็กทรอนิกส์ ซึ่งประกอบด้วย 3 มิติย่อยคือ ลักษณะการสื่อสารแบบบอกต่อ ทัศนคติของผู้บริโภคต่อการสื่อสารแบบบอกต่อในธุรกิจอิเล็กทรอนิกส์ และคุณภาพของ

เว็บไซต์อิเล็กทรอนิกส์ที่ส่งผลต่อ (1) ความพึงพอใจของผู้บริโภคในธุรกิจอิเล็กทรอนิกส์ และ (2) ความภักดีของผู้บริโภคในธุรกิจอิเล็กทรอนิกส์ โดยใช้แบบสอบถามในการเก็บรวบรวมข้อมูลกับกลุ่มตัวอย่าง ซึ่งเป็นเพศชายและเพศหญิงที่มีอายุระหว่าง 18-34 ปี ในเขตกรุงเทพมหานคร และเป็นผู้ที่เคยซื้อสินค้าผ่านอิเล็กทรอนิกส์คอมเมิร์ซ ซึ่งในงานวิจัยนี้คือ เว็บไซต์ Lazada และโซเชียลคอมเมิร์ซ ซึ่งในงานวิจัยนี้คือร้านค้าใน Facebook ภายในระยะเวลา 6 เดือนที่ผ่านมา จำนวน 400 คน ผลการวิจัยพบว่า ปัจจัยการสื่อสารแบบบอกต่อทั้งลักษณะการสื่อสารแบบบอกต่อ ทัศนคติของผู้บริโภคต่อการสื่อสารแบบบอกต่อในธุรกิจอิเล็กทรอนิกส์ และคุณภาพของเว็บไซต์ในธุรกิจอิเล็กทรอนิกส์มีอิทธิพลต่อความพึงพอใจและความภักดีของผู้บริโภคในธุรกิจอิเล็กทรอนิกส์ในบริบทอิเล็กทรอนิกส์คอมเมิร์ซหรือเว็บไซต์ Lazada อย่างมีนัยสำคัญทางสถิติ ขณะที่ในบริบทโซเชียลคอมเมิร์ซหรือร้านค้าใน Facebook มีปัจจัยการสื่อสารแบบบอกต่อเพียง 2 มิติย่อยที่มีอิทธิพลต่อความพึงพอใจและความภักดีของผู้บริโภคในธุรกิจอิเล็กทรอนิกส์ อย่างมีนัยสำคัญทางสถิติ

ฐิติมา อินกล่ำ (2558) ได้ศึกษาวาทกรรมทางการสื่อสารเพื่อการหลอกลวงทำธุรกรรมทางการเงินออนไลน์ผ่านเครื่องอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อศึกษา 1) ลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่างที่ถูกหลอกลวงทำธุรกรรมทางการเงินออนไลน์ผ่านเครื่องอิเล็กทรอนิกส์ 2) พฤติกรรมการถูกหลอกลวงทำธุรกรรมทางการเงินออนไลน์ 3) องค์ประกอบของวาทกรรมที่มีผลต่อการถูกหลอกลวงทำธุรกรรมทางการเงิน และ 4) ผลกระทบจากการถูกหลอกลวงในด้านจิตใจ สุขภาพ เศรษฐกิจ ครอบครัว และสังคม ศึกษาจากกลุ่มตัวอย่างที่ถูกหลอกลวงทำธุรกรรมทางการเงินออนไลน์ผ่านเครื่องอิเล็กทรอนิกส์ ในเขตพื้นที่จังหวัดอุตรดิตถ์ จำนวน 16 คน โดยแบ่งเป็นกลุ่มตัวอย่างที่มีมูลค่าความเสียหายน้อยกว่า 100,000 บาท จำนวน 8 คน และกลุ่มตัวอย่างที่มีมูลค่าความเสียหายตั้งแต่ 100,000 บาทขึ้นไป จำนวน 8 คน เก็บข้อมูลโดยการสัมภาษณ์เชิงลึก ผลการศึกษาสรุปได้ดังนี้ กลุ่มตัวอย่างทั้งหมดจำนวน 16 คน เป็นเพศหญิง 10 คน เพศชาย 6 คน อายุสูงสุด 73 ปี ต่ำสุด 20 ปี ส่วนใหญ่จบการศึกษาระดับปริญญาตรี มีรายได้เฉลี่ย 29,000 บาท/เดือน รายได้สูงสุดคือ 50,000 บาท/เดือน และรายได้ต่ำสุดคือ 6,000 บาท/เดือน มีอาชีพรับราชการ ทำธุรกิจ พนักงานเอกชน เกษตรกร และนักศึกษา ด้านการสมรสพบว่า 12 คนสมรสแล้ว ส่วนอีก 4 คนมีสถานภาพโสด โดยมีองค์ประกอบของวาทกรรมที่มีผลต่อการถูกหลอกลวงทำ

ธุรกรรมทางการเงินออนไลน์ผ่านเครื่องอิเล็กทรอนิกส์ ประกอบด้วย 3 ปัจจัย คือ 1) ปัจจัยด้านความน่าเชื่อถือของผู้ส่งสาร (มิจฉาชีพ) โดยการอ้างอิงเป็นบุคคลสำคัญ ได้แก่ อ้างเป็นเจ้าหน้าที่ธนาคาร เจ้าหน้าที่ตำรวจ เจ้าหน้าที่ DSI เจ้าหน้าที่ธนาคารแห่งประเทศไทย และเจ้าหน้าที่กรมสรรพากร โดยการสร้างความน่าเชื่อถือและไว้วางใจ ได้แก่ การใช้เสียงระบบอัตโนมัติแจ้งว่าเป็นหนี้บัตรเครดิต สร้างเรื่องให้ตนเองดูน่าเชื่อถือ อ้างถึงตำแหน่ง หน้าที่การงาน การอ้างอิงเกี่ยวกับระบบอิเล็กทรอนิกส์ ได้แก่ การได้รับรางวัลจากการสุ่มเบอร์โทร 2) ปัจจัยด้านเนื้อหาและวาทกรรม ประกอบด้วยการใช้วาทกรรมในการสร้างความสนใจ อาจเป็นเนื้อหาที่สร้างความหวาดกลัว ได้แก่ การบอกว่าเป็นหนี้บัตรเครดิต บัญชีหมุนเวียนผิดปกติเข้าข่ายการฟอกเงิน ถูกโจรกรรมข้อมูลบัญชี หรือวาทกรรมการสร้างความคาดหวัง ได้แก่ บอกว่าเป็นผู้โชคดีได้รับรางวัล ได้โปรโมชั่นจูงใจ ได้สินค้าราคาถูก ได้รับเงินภาษีคืน ได้รับเงินโอนจากต่างประเทศ จากนั้นจะใช้วาทกรรมในการกระตุ้นความต้องการและตอบสนองความต้องการของเหยื่อในด้านผลประโยชน์ ได้แก่ เป็นผู้ดูแลคดีจะให้ความช่วยเหลือ หวังว่าจะได้ร่วมงานกัน เพื่อความปลอดภัยของเงินในบัญชี ด้านการได้รับผลตอบแทนที่สูงกว่า ได้แก่ ให้บอกหมายเลขบัญชีเพื่อรับเงินรางวัล ได้ของดีราคาถูก จะช่วยให้รับเงินโอนเร็วขึ้น และด้านกฎหมาย ได้แก่ ช่วยเรื่องคดีฟอกเงิน คดีอาญา การถูกดำเนินคดี จากนั้นจะใช้วาทกรรมในการทำให้เห็นภาพด้านลบหรือด้านบวกจากการเชื่อและทำตาม และลำดับสุดท้ายจะใช้วาทกรรมในการทำให้เกิดการลงมือปฏิบัติ 2 รูปแบบคือ การข่มขู่ โดยจะอ้างในเรื่องของกฎหมาย การดำเนินคดี และการโน้มน้าว ได้แก่ ขอให้เหยื่อไปตรวจสอบยอดเงินโอน รับเงินรางวัล ตรวจสอบรายการบัญชี เพื่อแก้ไขระบบหรือป้องกันการโจรกรรมข้อมูล โอนเงินเพื่อซื้อสินค้าราคาถูก และ 3) ปัจจัยบริบทของผู้รับสาร ได้แก่ บริบทด้านสถานการณ์ หรือเงื่อนไขเวลา เป็นสิ่งที่กำหนดให้ผู้รับสารต้องรีบตัดสินใจในการทำธุรกรรมทางการเงิน ด้านจิตวิทยา เช่น ความกลัว ความโลภ อำนาจทางกฎหมาย รวมถึงวัฒนธรรม สังคม เศรษฐกิจส่วนตัวของผู้รับสารหรือเหยื่อเป็นสิ่งสำคัญที่ส่งผลให้เหยื่อหลงเชื่อกลอุบายของมิจฉาชีพ และกำหนดพฤติกรรมในการตัดสินใจทำธุรกรรมทางการเงิน

สุทธิรักส์ ศุขเขษม (2563) ได้ศึกษาเรื่องปัจจัยทางบุคลิกภาพที่มีผลต่อความเสี่ยงในการโจมตีด้วยระบบสารสนเทศด้วยวิศวกรรมสังคม โดยทำการศึกษาความสัมพันธ์ของบุคลิกภาพ 4 ด้านตามแบบทดสอบ MBTI ได้แก่ บุคลิกใช้ความคิด (Thinking) กับบุคลิกใช้ความรู้สึก (Feeling)

บุคลิกตัดสิน (Judging) กับบุคลิกรับรู้ (Perceiving) บุคลิกแสดงตัว (Extroversion) บุคลิกเก็บตัว (Introversion) และบุคลิกใช้ประสาทสัมผัส (Sensing) กับบุคลิกหยั่งรู้ (Intuition) รวมถึงปัจจัยด้านเพศ และการทำงานด้านเทคโนโลยีสารสนเทศ พิจารณากับปัจจัยที่ผู้โจมตีใช้หลักทางจิตวิทยาในการชักจูงผู้ใช้ให้กระทำการให้เกิดความเสียหายแก่ระบบสารสนเทศหรือวิศวกรรมสังคม (Social Engineering) 3 ด้าน ได้แก่ ความอยากรู้อยากเห็น (Curiosity) ความกลัว (Fear) และความโลภ (Greedy) มีผู้ตอบแบบสอบถามจากทั้ง 4 วิทยาเขต จำนวน 53 คน เป็นเพศชายจำนวน 24 คน เพศหญิงจำนวน 29 คน เป็นคนที่ทำงานทางด้านเทคโนโลยีสารสนเทศ 21 คน และไม่ได้ทำงานด้านเทคโนโลยีสารสนเทศ 32 คน บุคลิกใช้ความคิด จำนวน 32 คน บุคลิกใช้ความรู้สึก จำนวน 21 คน บุคลิกตัดสิน จำนวน 21 คน บุคลิกรับรู้ จำนวน 32 คน บุคลิกแสดงตัว 32 คน บุคลิกเก็บตัว จำนวน 21 คน บุคลิกใช้ประสาทสัมผัสจำนวน24 คน และบุคลิกหยั่งรู้ จำนวน 29 คน จากการวิจัยนี้ได้ข้อสรุปว่าผู้ใช้ที่มีบุคลิกตัดสินมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมสังคมจากความอยากรู้อยากเห็นมากกว่าบุคลิกรับรู้ และผู้ใช้ที่มีบุคลิกตัดสินมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมสังคมจากความกลัวมากกว่าบุคลิกรับรู้ บุคลิกใช้ความคิดมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมสังคมจากความกลัวมากกว่าบุคลิกใช้ความรู้สึก เพศชายมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมสังคมจากความโลภมากกว่าเพศหญิง คนทำงานด้านเทคโนโลยีสารสนเทศมีโอกาสที่จะถูกชักจูงด้วยวิศวกรรมสังคมจากความกลัวน้อยกว่าคนที่ไม่ได้ทำงานด้านเทคโนโลยีสารสนเทศ อย่างมีนัยสำคัญ

ปวีณา ชัยวนารมย์ (2558) ได้ศึกษาการพัฒนาแบบจำลองเพื่อพยากรณ์โอกาสการเกิดความเครียดในหลายระดับด้วยเทคนิคการทำเหมืองข้อมูล โดยมีวัตถุประสงค์เพื่อศึกษาหาแบบจำลองที่เหมาะสมสำหรับพยากรณ์ความเครียดด้วยเทคนิคการทำเหมืองข้อมูล กระบวนการวิจัยเริ่มต้นด้วยให้กลุ่มตัวอย่างจำนวน 300 คน ทำแบบทดสอบประเมินความเครียดเป็นจำนวน 4 รอบ โดยแต่ละรอบการประเมินมีระยะห่างของการทำแบบทดสอบเป็นระยะเวลา 2 เดือน จากนั้น ผลการทำสอบที่ได้ทั้งหมดถูกป้อนเข้าสู่โปรแกรม WEKA เพื่อทำการสร้างแบบจำลองด้วยอัลกริทึมทางด้านเหมืองข้อมูลจำนวน 6 อัลกอริทึม คือ Bayesian Network, Naïve Bayesian, Decision Tree: 4.5, Decision Table, Partial Rules (PART) และ Multilayer Perceptron (MLP) ในการสร้างแบบจำลองและการทดสอบแบบจำลองนั้น วิธี 10-fold cross-validation ได้ถูกนำมาใช้ในการแบ่งข้อมูลออกเป็นสองชุด ได้แก่ ชุดข้อมูลสอนและชุดข้อมูลทดสอบ จากการ

ทดสอบแบบจำลองทั้งหมดพบว่า แบบจำลองที่เหมาะสมที่สุดในการนำมาใช้เพื่อพยากรณ์ความเครียดคือ แบบจำลองที่สร้างจากอัลกอริทึม MLP ที่ใช้กับข้อมูลย้อนหลัง 6 เดือน โดยแบบจำลองนี้ มีค่าความถูกต้อง ค่าความแม่นยำ ค่าความระลึก และค่าความเหวี่ยง เท่ากับ ร้อยละ 81, 0.81, 0.81 และ 0.81 ตามลำดับ

Aburrous (2010) ได้ศึกษาการพยากรณ์เว็บไซต์ฟิชชิ่งด้วยเทคนิคเหมืองข้อมูล ผลการศึกษาพบว่าโมเดลที่พัฒนาขึ้นจากเทรนด์ข้อมูลเกี่ยวกับฟิชชิ่ง 6 ประเภท ได้แก่ โดเมนเว็บไซต์, การตั้งค่าความปลอดภัยของเว็บไซต์, โค้ดที่ใช้เขียนเว็บไซต์, เนื้อหา, ช่องกรอกเว็บไซต์ และ ปัจจัยส่วนบุคคล มีประสิทธิภาพในการทำนาย ตรวจจับ และคาดการณ์เว็บไซต์ที่เป็นฟิชชิ่งได้ในระดับสูง นอกจากนี้ผลการทดลองยังแสดงให้เห็นถึงความเป็นไปได้ของการใช้เทคนิคการจำแนกแบบความสัมพันธ์ (Associative Classification) สำหรับตรวจจับเว็บไซต์หลอกลวง

Pandey Mayank (2013) ได้ศึกษา การตรวจจับฟิชชิงและสแปมโดยใช้ชุดข้อความและวิธีการเหมืองข้อมูล ผลการวิจัยพบว่าโมเดลที่สร้างขึ้นโดยอาศัยคุณลักษณะ 17 ประการจากซอร์สโค้ดและ URL ของเว็บไซต์ มีประสิทธิภาพสูงเมื่อเทียบกับการศึกษาในครั้งก่อน

จากการศึกษาทฤษฎีและงานวิจัยที่เกี่ยวข้องในอดีต พบว่า ปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล นั้นประกอบด้วย

ตารางที่ 2.10 ตัวแปรที่กล่าวถึงในงานวิจัยที่เกี่ยวข้อง

ลำดับ	ผู้เขียน	ชื่อเรื่อง	แหล่งข้อมูล	สิ่งที่ค้นพบ
1	Information Gap Theory (1994)	Information Gap Theory	Sciencedirect	ความอยากรู้อยากเห็น และการตัดสินใจ ขับเคลื่อนเหมือนกับสภาวะอื่น ๆ เช่น ความหิว
2	Ahmed & Omotunde (2012)	Theories and strategies of good decision making	IJSTR	ประสบการณ์และทักษะการวิเคราะห์ปัญหาที่ดีส่งผลให้เกิดการตัดสินใจที่ดีขึ้น
3	Ainslie (1975)	Specious reward: a behavioral theory of impulsiveness and impulse control	APA PsycArticles	ความคุ้นชินกับการตอบสนองรูปแบบเดิมส่งผลให้เกิดความหุนหันพลันแล่น

ตารางที่ 2.10 ตัวแปรที่กล่าวถึงในงานวิจัยที่เกี่ยวข้อง (ต่อ)

ลำดับ	ผู้เขียน	ชื่อเรื่อง	แหล่งข้อมูล	สิ่งที่ค้นพบ
4	Birkett (2017)	Fear and Greed: What Drives Human Behavior?	CXL	ความกลัวและความโลภส่งผลต่อการโน้มน้าวให้ลูกค้าคลิกซื้อสินค้าบนโลกออนไลน์
5	Breda & Berlamont (2014)	The secret of fear and greed behind financial decision making	Ghent University	ผู้ชาย มีปัจจัยด้านความโลภและความกลัว ทำให้ตัดสินใจด้านการเงินได้ไม่ดีเท่าผู้หญิง
6	Dijkstra (2018)	Relation between Dispositional Greed and Impulsive Buying Tendency: Role of Cognitive Reflection	Tilburg University	ความโลภมีความสัมพันธ์เชิงบวกต่อการทำให้เกิดความอยากซื้อที่หุนหันพลันแล่น
7	Golman & Loewenstein (2015)	Curiosity, information gaps, and the utility of knowledge	Carnegie Mellon University	ความคาดหวังของผู้รับสารส่งผลต่อการรับรู้และยอมรับข้อมูลของผู้รับสารเอง
8	Hooper & Blunt (2020)	Factors influencing the information security behavior of IT employees	Taylor & Francis	ความเชื่อในความสามารถของตนเองและการรับรู้ถึงผลกระทบที่อาจเกิดขึ้นมีผลแปรผันต่อพฤติกรรมของผู้รับสาร
9	House & Raja (2020)	Phishing: message appraisal and the exploration of fear and self-confidence	Taylor & Francis	ความกลัวส่งผลให้ความอยากที่จะกระทำและการกระทำลดลง แต่ความมั่นใจในตนเองจะเพิ่มความอยากที่จะกระทำให้มากขึ้น
10	Jansen & van Schaik (2019)	Design and evaluation of a theory-based intervention to promote security behaviour against phishing	ScienceDirect	การจูงใจด้วยความกลัวช่วยเพิ่มความตระหนักต่อการป้องกันการถูกล่อลวง
11	Musuva, Getao & Chepken (2019)	A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility	ScienceDirect	ความสามารถในการระบุภัยการล่อลวงของผู้รับสารมีผลแปรผกผันต่อการเป็นตกเหยื่อของภัยการล่อลวง

ตารางที่ 2.10 ตัวแปรที่กล่าวถึงในงานวิจัยที่เกี่ยวข้อง (ต่อ)

ลำดับ	ผู้เขียน	ชื่อเรื่อง	แหล่งข้อมูล	สิ่งที่ค้นพบ
12	Albladi & George (2017)	Personality traits and cyber-attack victimisation: Multiple mediation analysis	IEEE	จากลักษณะบุคลิกภาพ 5 อย่าง ปัจจัยความสนใจต่อสิ่งภายนอกส่งผลเชิงบวก แต่ปัจจัยความพิถีพิถัน ความยินยอมเห็นใจ และความไม่เสถียรทางอารมณ์ ส่งผลเชิงลบต่อการตกเป็นเหยื่อภัยไซเบอร์
13	Jansen, J. & Van Schaik (2018)	Testing a model of precautionary online behaviour: The case of online banking	ScienceDirect	ความเชื่อมั่นในประสิทธิภาพของมาตรการการป้องกันและความสามารถของบุคคลที่จะปฏิบัติตาม เป็นตัวแปรสำคัญในการป้องกันจากการถูกล่อลวง
14	Sharp & Wu (2017)	Student Intentions and Behaviors Related to Email Security: An Application of the Health Belief Model	JISAR	ความคาดหวังและความเชื่อในความสามารถตนเองมีความสัมพันธ์อย่างชัดเจนกับพฤติกรรมการระวังภัยการโจมตีทางอีเมล
15	Wang & Rao (2017)	Coping responses in phishing detection: an investigation of antecedents and consequences	INFORMS	ความยืดหยุ่นในการรับมือจากภัยล่อลวงมีผลเชิงบวกต่อความพยายามและความแม่นยำของการระบุอีเมลลวง
16	ArachcilageLove & Benznosov (2016)	Phishing threat avoidance behaviour: An empirical investigation	ScienceDirect	ความสามารถในการสังเกตที่อยู่ของเว็บไซต์ ช่วยเพิ่มความปลอดภัยจากการล่อลวงทางเว็บไซต์
17	Harrison, Svetieva & Vishwanath (2016)	Individual processing of phishing emails	Emerald	ความใส่ใจ ความรู้ และประสบการณ์ ส่งผลเชิงลบต่อความเสี่ยงในการถูกล่อลวงทางอีเมล ความน่าเชื่อถือของเนื้อหาส่งผลเชิงบวกต่อการถูกล่อลวงทางอีเมล

ตารางที่ 2.10 ตัวแปรที่กล่าวถึงในงานวิจัยที่เกี่ยวข้อง (ต่อ)

ลำดับ	ผู้เขียน	ชื่อเรื่อง	แหล่งข้อมูล	สิ่งที่ค้นพบ
18	Alseadoon, Ibrahim & Oihman (2015)	What is the influence of users' characteristics on their ability to detect phishing emails?	Proceedings of the 1st International Conference on Communication and Computer Engineering	ความสนใจต่อสิ่งภายนอก ความเชื่อใจ และความอ่อนน้อมถ่อมตนมีความสัมพันธ์เชิงลบ ต่อความตระหนักถึงภัยอีเมล
19	Halevi, Memon & Nov (2015)	Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks	SSRN	บุคลิกด้านความพิถีพิถันมีความสัมพันธ์เชิงบวกต่อการถูกล่อลวง
20	Harrison, Vishwanath & Rao (2015)	Examining the impact of presence on individual phishing victimization	IEEE	คุณภาพของเนื้อหาในอีเมลลวงมีความสัมพันธ์เชิงบวกต่อการถูกล่อลวงของผู้รับอีเมล
21	Reyns (2015)	A routine activity perspective on online victimisation	Emerald	ปริมาณการทำธุรกรรมของบุคคลส่งผลเชิงบวกต่อการถูกล่อลวง
22	Leukfeldt & Yar (2014)	Applying routine activity theory to cybercrime: A theoretical and empirical analysis	Taylor & Francis	พฤติกรรม ความเชื่อ ผู้ส่ง และกิจกรรมออนไลน์ส่งผลต่อการถูกล่อลวง
23	Purkait (2014)	An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website	Emerald	ความระแวดระวัง ประสบการณ์ อายุ และความจำระยะสั้นมีความสัมพันธ์เชิงบวกต่อการรู้ถึงภัยการล่อลวง
24	Luo, Zhang, Burd & Seazzu (2013)	Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration	ScienceDirect	แบบจำลองด้านทฤษฎีการล่อลวงพบว่าผู้คนมักจะละเลยและตัดสินใจที่ไม่เหมาะสมเกี่ยวกับความมั่นคงบนระบบไอที
25	Yoon & Kim (2013)	Understanding computer security behavioral intention in the workplace	Emerald	ศีลธรรม วัฒนธรรมองค์กร และมุมมองต่อความปลอดภัยทางคอมพิวเตอร์มีความสัมพันธ์กับความเสี่ยงจากการถูกโจมตี

ตารางที่ 2.10 ตัวแปรที่กล่าวถึงในงานวิจัยที่เกี่ยวข้อง (ต่อ)

ลำดับ	ผู้เขียน	ชื่อเรื่อง	แหล่งข้อมูล	สิ่งที่ค้นพบ
26	Pattinson, Jerram, Parsons, Mccormac & Butavicius (2012)	Why do some people manage phishing e-mails better than others?	Emerald	บุคคลจะมีการตอบสนองและจัดการต่ออีเมลลวงได้ย่ำแย่กว่าอีเมลปกติ
27	Wang (2012)	Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email	IEEE	การตอบสนองต่อสิ่งเร้าโดยสัญชาตญาณส่งผลเชิงบวกต่อการตอบสนองต่ออีเมลลวง
28	Ngo & Paternoster (2011)	Cybercrime Victimization: An examination of Individual and Situational level factors	University of South Florida	ปัจจัยส่วนบุคคลและสถานการณ์ที่เกิดขึ้นรอบตัว มีผลต่อการเพิ่มโอกาสในการตกเป็นเหยื่อล่อลวง
29	Vishwanath, Herath, Chen, Wang, & Rao (2011)	Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model	ScienceDirect	เนื้อหาที่แสดงถึงความต้องการความเร่งด่วนในการตอบอีเมลมีผลเชิงบวกต่อการตกเป็นเหยื่อในการล่อลวงทางอีเมล
30	Parrish, Bailey & Courtney (2015)	A personality based model for determining susceptibility to phishing attacks	University of Arkansas at Little Rock	บุคลิกด้านความพิถีพิถันมีความสัมพันธ์เชิงลบต่อการถูกล่อลวง แต่ความสนใจต่อสิ่งภายนอกมีความสัมพันธ์เชิงบวกต่อการถูกล่อลวง
31	Sheng, Holbrook, Kumaraguru, Cranor & Downs (2010)	Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions	ACM	ผู้หญิงมีแนวโน้มที่จะตกเป็นเหยื่อการล่อลวงมากกว่าผู้ชาย และกลุ่มช่วงอายุ 18-25 ปี มีแนวโน้มที่จะตกเป็นเหยื่อการถูกล่อลวงมากกว่าช่วงอายุอื่น
32	Wright & Marett (2010)	The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived	Taylor & Francis	ประสบการณ์และการเรียนรู้ถึงภัยการล่อลวงช่วยลดความเสี่ยงจากการตกเป็นเหยื่อการถูกล่อลวง

ตารางที่ 2.10 ตัวแปรที่กล่าวถึงในงานวิจัยที่เกี่ยวข้อง (ต่อ)

ลำดับ	ผู้เขียน	ชื่อเรื่อง	แหล่งข้อมูล	สิ่งที่ค้นพบ
33	Hill, Fombelle & Sirianni (2016)	Shopping under the influence of curiosity: How retailers use mystery to drive purchase motivation	ScienceDirect	ความอยากรู้อยากลอง ส่งผลให้ลูกค้าตัดสินใจซื้อสินค้า โดยที่ไม่ทราบถึงข้อมูล รายละเอียดสินค้าที่แน่ชัด
34	Kahneman (2011)	Thinking, fast and slow	Doubleday Canada	มนุษย์ไม่ได้มีชุดความคิดแบบซับซ้อนทำให้เกิดการตัดสินใจที่ผิดบ่อยครั้ง
35	Laran & Tsiros (2013)	An investigation of the effectiveness of uncertainty in marketing promotions involving free gifts	American Marketing Association – Journal of Marketing	เมื่อมีตัวเลือกให้ตัดสินใจโดยมีความไม่แน่นอนเข้ามาเกี่ยวข้อง การตัดสินใจโดยใช้ความรู้สึก ช่วยเพิ่มความน่าจะเป็นในการซื้อของลูกค้า
36	Litman & Spielberger (2003)	Measuring Epistemic Curiosity and Its Diversive and Specific Components	Taylor & Francis	ความอยากรู้อยากเห็นนำมาซึ่งความวิตกกังวลและความกลัว โดยพบผู้ชายมีแนวโน้มเสี่ยงสูงกว่า
37	Mussel et al. (2015)	State- and trait-greed, its impact on risky decision-making and underlying neural mechanisms	Taylor & Francis	ความโลภมีความสัมพันธ์กับความกล้าเสี่ยงในการพนัน
38	Sakaki, Yagi & Murayama (2018)	Curiosity in old age: A possible key to achieving adaptive aging	ScienceDirect	อายุมีความสัมพันธ์เชิงลบต่อความอยากรู้อยากเห็น
39	Seuntjens et al. (2015)	Defining greed	The British Psychological Society	ความโลภสามารถตีความได้หลายมุมมองเช่น เป็นแรงผลักดันให้มุ่งมานะขวนขวาย หรือเป็นความเห็นแก่ตัว
40	Spielberger (2004)	Encyclopedia of applied psychology	Encyclopedia of applied psychology	ปัจจัยด้านจิตวิทยา มีอิทธิพลต่อพฤติกรรมและการกระทำของมนุษย์

ตารางที่ 2.10 ตัวแปรที่กล่าวถึงในงานวิจัยที่เกี่ยวข้อง (ต่อ)

ลำดับ	ผู้เขียน	ชื่อเรื่อง	แหล่งข้อมูล	สิ่งที่ค้นพบ
41	Limandri (1998)	Psychiatric-mental health nurse practitioner with expertise in violence against women and substance abuse	Taylor & Francis	ความอับอาย ความกลัวถูกปิดบังไม่ให้คนอื่นทราบ นำไปสู่การมีปัญหาเรื้อรัง ไม่สามารถแก้ไขได้อย่างง่าย
42	ชานนท์ สำเภาอินทร์ (2557)	ความรับผิดในการขู่เข็ญให้ผู้อื่นเกิดความกลัว	มหาวิทยาลัยธรรมศาสตร์	การทำให้ผู้อื่นเกิดความกลัว เป็นการละเมิดความมั่นคงปลอดภัยในชีวิตของมนุษย์
43	เบญจพร ลิ้มธรรมาภรณ์ (2554)	การตรวจจับบอทเน็ตสแปมเมล์และความตระหนักในภัยลวงเฟซบุ๊คฟิชชิ่ง	มหาวิทยาลัย เทคโนโลยีพระจอมเกล้าพระนครเหนือ	การสังเกตที่อยู่ของเว็บไซต์และที่อยู่ของผู้ส่งอีเมล สามารถชะลอความเสี่ยงและป้องกันภัยอีเมลลวงได้
44	สุรชัย ฉัตรเฉลิมพันธุ์ (2563)	ความมั่นคงปลอดภัย: กรณีศึกษาการรู้เท่าทันภัยทางไซเบอร์ของผู้บริหารในสถาบันการเงินโดยการจำลองการโจมตีด้วยฟิชชิ่ง	วารสารวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยธนบุรี	การทดลองการโจมตีทางไซเบอร์ พบว่ากลุ่มตัวอย่างหลงเชื่ออีเมลปลอม เพราะอ้างเป็นองค์กรและบุคคลที่น่าเชื่อถือ
45	ปวันตา บุญพันธ์ (2557)	การศึกษาความรู้สึกหวาดกลัวอาชญากรรมของผู้สูงอายุในเขตลาดพร้าว กรุงเทพมหานคร	มหาวิทยาลัยธรรมศาสตร์	ความหวาดกลัว ความกังวล สามารถบรรเทาได้ด้วยความคาดหวังว่าจะมีสิ่งให้พึ่งพา ไว้วางใจได้
46	สุดารัตน์ วงศ์คำ (2550)	การศึกษาวิเคราะห์คำสอนเรื่องโลภะในพระพุทธศาสนาเถรวาท	มหาวิทยาลัยธรรมศาสตร์	ความโลภ เป็นสิ่งที่ทำให้มนุษย์เกิดพฤติกรรมเสี่ยง
47	ฐิติมา อินกล่ำ (2558)	วาทกรรมทางการสื่อสารเพื่อการหลอกลวงทางธุรกรรมทางการเงินออนไลน์ ผ่านเครื่องอิเล็กทรอนิกส์	มหาวิทยาลัยราชภัฏอุตรดิตถ์	ความน่าเชื่อถือ ทักษะการโน้มน้าวของผู้ส่งสาร และบริบทของผู้รับสารที่สุ่มเสี่ยงต่อการชักจูง ล้วนเพิ่มโอกาสในการถูกล่อลวง ทำให้เสียทรัพย์
48	ตฤณ ทวิธารานนท์ (2562)	บทบาทของโซเชียลมีเดียในการลงโทษทางสังคม	มหาวิทยาลัยรังสิต	โซเชียลมีเดียเป็นตัวช่วยในการขยายการสื่อสารออกไปในวงกว้าง

ตารางที่ 2.10 ตัวแปรที่กล่าวถึงในงานวิจัยที่เกี่ยวข้อง (ต่อ)

ลำดับ	ผู้เขียน	ชื่อเรื่อง	แหล่งข้อมูล	สิ่งที่ค้นพบ
49	สุนันทา เรียงแหลม (2551)	การศึกษาแก้ปัญหาความโลภในสังคมปัจจุบันตามหลักพระพุทธศาสนาเถรวาท	วารสารปัญญาปณิธาน	ความโลภ เป็นสาเหตุที่ทำให้เกิดพฤติกรรมอันตรายตามมา
50	พงศ์พนธ์ ภาวศุทธิ์ (2561)	สาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ของกลุ่ม เจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล	มหาวิทยาลัยธรรมศาสตร์	อารมณ์และความรู้สึกต่าง ๆ ส่งผลให้ผู้ถูกโจมตีตัดสินใจอย่างไม่มีเหตุผลและถูกโจมตีในที่สุด

บทที่ 3

วิธีดำเนินการวิจัย

การวิจัยเรื่อง “การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล” เป็นการวิจัยและพัฒนา (Research and Development) โดยผู้วิจัยดำเนินการศึกษาค้นคว้าโดยมีขั้นตอนดังต่อไปนี้

3.1 ประชากรและกลุ่มตัวอย่าง

3.2 วิธีการสุ่มตัวอย่าง

3.3 เครื่องมือที่ใช้ในการรวบรวมข้อมูล

3.4 วิธีการเก็บรวบรวมข้อมูล

3.5 สถิติที่ใช้และการพัฒนาแบบจำลอง

3.1 ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการวิจัยครั้งนี้ คือ ผู้รับสารกลุ่มดิจิทัลเนทีฟไทย ซึ่งหมายถึง บุคคลที่มีอายุระหว่าง 18 - 36 ปี ทั้งเพศชายและเพศหญิง และใช้งานอินเทอร์เน็ตเป็นประจำอย่างน้อย 5 ปี ติดต่อกัน ซึ่งมีจำนวนทั้งสิ้น 4,387,062 คน (ITU 2013, อ้างถึงใน ศุภกร จูฑะพล, 2557)

สำหรับกลุ่มตัวอย่างในการวิจัย ผู้วิจัยได้กำหนดขนาดตัวอย่างจากคำนวณขนาดกลุ่มตัวอย่างตามสูตรของ Cochran (1963 อ้างถึงใน กษิดิศ สตางค์มงคล, 2562) โดยกำหนดค่าความเชื่อมั่น (Confidence level) ของกลุ่มตัวอย่างที่ร้อยละ 95 ค่าสัดส่วนของประชากรที่ผู้วิจัยต้องการ .5 และค่าความคลาดเคลื่อนที่ยอมรับได้ไม่เกินร้อยละ 0.03 ดังแสดงในสมการต่อไปนี้

$$n_0 = \frac{z^2 p(1\text{-}p)}{e^2}$$

เมื่อ n_0 แทน จำนวนตัวอย่าง

z แทน ระดับความเชื่อมั่น

p แทน สัดส่วนของประชากรที่ผู้วิจัยต้องการ

e แทน ค่าความคลาดเคลื่อน

ผู้วิจัยนำข้อมูลมาแทนค่าในสูตรดังกล่าวจะได้เป็น

$$n_0 = \frac{(1.96^2)(.5)(1\text{-}.5)}{.03^2}$$
$$n_0 = \frac{0.9604}{.0009}$$
$$n_0 = 1{,}067.1 \approx 1{,}068$$

เนื่องจากผู้วิจัยทราบจำนวนประชากรทั้งหมดจึงนำค่า n_0 จากสมการข้างต้นเข้ากระบวนการ Finite Population Correction เพื่อคำนวณขนาดกลุ่มตัวอย่าง ดังแสดงวิธีทำตามสมการต่อไปนี้

$$n = \frac{n_0}{1 + \frac{(n_0\text{-}1)}{N}}$$

เมื่อ n_0 แทน จำนวนตัวอย่าง

n แทน ขนาดของกลุ่มตัวอย่าง

N แทน ประชากรทั้งหมด

ผู้วิจัยนำข้อมูลมาแทนค่าในสูตรดังกล่าวจะได้เป็น

$$n = \frac{1{,}068}{1+\frac{(1{,}068\text{-}1)}{4{,}387{,}062}}$$

$$n = \frac{1{,}068}{1.00024298722}$$

$$n = 1{,}066.74 \approx 1{,}067$$

ดังนั้นควรเก็บกลุ่มตัวอย่างทั้งสิ้น 1,067 ตัวอย่าง

3.2 วิธีการสุ่มตัวอย่าง

ในการวิจัยครั้งนี้ ผู้วิจัยได้ทำการสุ่มตัวอย่างแบบหลายขั้นตอน (Multi-stage sampling) โดยใช้วิธีการสุ่มตัวอย่างทั้งแบบที่อาศัยความน่าจะเป็น (Probability Sampling) และแบบที่ไม่อาศัยความน่าจะเป็น (Non-probability sampling) ซึ่งมีรายละเอียดดังต่อไปนี้

ขั้นตอนที่ 1 การสุ่มตัวอย่างแบบโควตา (Quota sampling)

กรมการปกครอง กระทรวงมหาดไทย ได้แบ่งภูมิศาสตร์ของประเทศไทยออกเป็น 4 ภาค ได้แก่ ภาคกลาง ประกอบด้วย 26 จังหวัด ภาคตะวันออกเฉียงเหนือ (อีสาน) ประกอบด้วย 20 จังหวัด ภาคใต้ ประกอบด้วย 14 จังหวัด และ ภาคเหนือ ประกอบด้วย 17 จังหวัด ผู้วิจัยจึงใช้หลักเกณฑ์ทางภูมิศาสตร์เป็นตัวตั้งต้นในวิธีการสุ่มตัวอย่าง

ตารางที่ 3.1 จำนวนจังหวัดในประเทศไทยแยกตามภูมิภาค

ภูมิภาค	จำนวนจังหวัด
กลาง	26
ตะวันออกเฉียงเหนือ	20
ใต้	14
เหนือ	17
รวม	**77**

ขั้นตอนที่ 2 การสุ่มตัวอย่างแบบง่าย (Simple random sampling)

ผู้วิจัยได้ทำการสุ่มตัวอย่างแบบง่ายโดยการเขียนชื่อจังหวัดทั้ง 77 จังหวัด ลงในกระดาษ 77 ใบ หลังจากนั้นนำรายชื่อจังหวัดต่าง ๆ หย่อนลงกล่องโดยแบ่งออกเป็นภูมิภาคต่าง ๆ ครบทั้ง 4 ภูมิภาค แล้วจึงจับสลากออกมาเป็นจำนวนครึ่งหนึ่งจากจำนวนสลากในภูมิภาคต่าง ๆ ยกเว้นภาคเหนือที่มีจำนวนจังหวัดหารไม่ลงตัว ผู้วิจัยจึงทำการจับสลากเพิ่มอีก 1 จังหวัด

โดยภาคกลาง จับสลากได้จังหวัด กรุงเทพฯ นนทบุรี ปทุมธานี นครปฐม สมุทรปราการ สมุทรสาคร สมุทรสงคราม สุพรรณบุรี อ่างทอง ระยอง ราชบุรี สระแก้ว และพระนครศรีอยุธยา

ภาคตะวันออกเฉียงเหนือ จับสลากได้จังหวัด ขอนแก่น กาฬสินธุ์ นครราชสีมา มหาสารคาม ยโสธร เลย ศรีสะเกษ สุรินทร์ อำนาจเจริญ และอุบลราชธานี

ภาคใต้ จับสลากได้จังหวัด ภูเก็ต กระบี่ นครศรีธรรมราช ปัตตานี พังงา พัทลุง และสงขลา

และภาคเหนือ จับสลากได้จังหวัด เชียงใหม่ น่าน พะเยา พิจิตร เพชรบูรณ์ แพร่ ลำพูน อุทัยธานี อุตรดิตถ์

ตารางที่ 3.2 จำนวนสลากที่สุ่มจับได้แยกตามจังหวัดต่าง ๆ

ภูมิภาค	**จำนวนจังหวัด**	**จำนวนสลากที่จับได้**
กลาง	26	13
ตะวันออกเฉียงเหนือ	20	10
ใต้	14	7
เหนือ	17	9
รวม	**77**	**39**

ขั้นตอนที่ 3 การสุ่มตัวอย่างแบบโควตา (Quota sampling)

ผู้วิจัยทำการคำนวณหาสัดส่วน (Proportion to size) ของกลุ่มตัวอย่าง เพื่อให้ได้กลุ่มตัวอย่างที่เป็นตัวแทนของประชากรทั้งประเทศโดยมีรายละเอียดดังนี้

ตารางที่ 3.3 จำนวนกลุ่มตัวอย่างที่สุ่มแบบโควตา

ภูมิภาค	จำนวนจังหวัด	จำนวนสลากที่จับได้	กลุ่มตัวอย่าง
กลาง	26	13	360
ตะวันออกเฉียงเหนือ	20	10	277
ใต้	14	7	194
เหนือ	17	9	236
รวม	**77**	**39**	**1,067**

ขั้นตอนที่ 4 การสุ่มตัวอย่างแบบเฉพาะเจาะจง (Purposive Sampling)

เมื่อได้ตัวแทนและขนาดของกลุ่มตัวอย่างที่ต้องการของแต่ละภูมิภาค ผู้วิจัยจึงทำการสุ่มตัวอย่างแบบเฉพาะเจาะจง โดยการสร้างแบบสอบถามออนไลน์ผ่าน Google Form และนำแบบสอบถามดังกล่าวไปโพสต์ในสื่อสังคมออนไลน์ พร้อมทั้งซื้อโฆษณาบนเฟซบุ๊ก โดยระบุเงื่อนไขของโฆษณาให้สอดคล้องกับกลุ่มเป้าหมายที่เป็นกลุ่มดิจิทัลเนทีฟ อาทิ พื้นที่ภูมิศาสตร์ในการเข้าถึงโฆษณา ระบุตามจังหวัดที่มีการจับสลากได้ในขั้นตอนที่ 2 ช่วงอายุที่เห็นโฆษณา กำหนดช่วงอายุ 18-36 ปี ตามประชากรหลักในการวิจัย เป็นต้น

3.3 เครื่องมือที่ใช้ในการรวบรวมข้อมูล

งานวิจัยนี้เป็นการวิจัยและพัฒนา (Research and Development) โดยใช้แบบสอบถามที่ประกอบด้วยสามส่วน ส่วนที่หนึ่งคือความหมายของการล่อลวงบนสื่อดิจิทัล ส่วนที่สองคือแบบสอบถามเพื่อการคัดเลือกกลุ่มตัวอย่าง (Screening Questionnaire) และส่วนที่สามแบบสอบถามหลัก (Main Questionnaire) โดยแบบสอบถามทั้งหมด มีรายละเอียดดังนี้

3.3.1 ความหมายของการล่อลวงบนสื่อดิจิทัล

แบบสอบถามในส่วนที่หนึ่ง ใช้เพื่ออธิบายความหมายของการล่อลวงบนสื่อดิจิทัล เพื่อให้ผู้ตอบแบบสอบถาม สามารถตอบได้ตรงกับความหมายที่ผู้วิจัยกำหนดไว้ในนิยามศัพท์

3.3.2 แบบสอบถามในการคัดกรองกลุ่มตัวอย่าง (Screening Questionnaire)

แบบสอบถามในส่วนที่สอง ใช้เพื่อคัดกรองกลุ่มตัวอย่างที่ตรงตามนิยาม Digital Native ตามนิยามศัพท์กำหนดไว้ คือ มีอายุระหว่าง 18-36 ปี และมีการใช้งานอินเทอร์เน็ตเป็นประจำอย่างน้อย 5 ปีติดต่อกัน เพื่อให้ได้กลุ่มตัวอย่างที่ตรงกับการวิจัย “การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยง ต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล” ดังนั้นผู้วิจัยจึงจัดทำคำถามในการคัดกรองกลุ่มตัวอย่าง จำนวนทั้งสิ้น 2 ข้อดังนี้

3.3.2.1 คุณมีอายุระหว่าง 18-36 ปี

3.3.2.2 คุณมีประสบการณ์การใช้งานอินเทอร์เน็ต 5 ปีขึ้นไป

3.3.3 แบบสอบถามหลัก (Main Questionnaire)

แบบสอบถามในส่วนที่สาม เพื่อให้กลุ่มตัวอย่างตอบคำถามสำหรับการวิจัยศึกษาเรื่อง “การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยง ต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล” ประกอบไปด้วยคำถาม 3 ตอนดังนี้

ตอนที่ 1 เป็นแบบสอบถามเกี่ยวกับข้อมูลลักษณะปัจจัยส่วนบุคคลของผู้ตอบแบบสอบถาม ลักษณะคำถามเป็นคำถามแบบเลือกตอบจากคำตอบที่กำหนดไว้ โดยจะเป็นคำถามเกี่ยวกับปัจจัยทางประชากรศาสตร์ ได้แก่ เพศ อายุ ระดับการศึกษา อาชีพ รายได้

ตอนที่ 2 เป็นแบบสอบถามเกี่ยวกับปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล ใช้ข้อคำถามซึ่งกำหนดคะแนนด้วยมาตรวัดของลิเคอร์ท (Likert scale) 5 ระดับ เห็นด้วยที่สุด เห็นด้วย ไม่แน่ใจ ไม่เห็นด้วย ไม่เห็นด้วยที่สุด ประกอบไปด้วยประเภทของข้อคำถาม 3 ประเภท ได้แก่ ผู้ส่งสาร สาร และผู้รับสาร ที่ผู้วิจัยประยุกต์จากการทบทวนแนวคิด และวรรณกรรมที่เกี่ยวข้องกับปัจจัยการสื่อสารและลักษณะเฉพาะของสารสนเทศ โดยมีเกณฑ์การเลือกตอบและให้น้ำหนักคะแนนดังตารางที่ 3.4

ตารางที่ 3.4 เกณฑ์การเลือกตอบและให้น้ำหนักคะแนน

คะแนน	ระดับความจริง
5	เห็นด้วยที่สุด
4	เห็นด้วย
3	ไม่แน่ใจ
2	ไม่เห็นด้วย
1	ไม่เห็นด้วยที่สุด

ด้านการแปลผลค่าเฉลี่ยที่ได้จากการเก็บข้อมูล จะใช้สูตรการคำนวณช่วงกว้างของอันตรภาคชั้นโดยแบ่งออกเป็น 5 ระดับ (วิเชียร เกตุสิงห์, 2538 อ้างถึงใน ประภัสสร ศรีสด, 2558) ดังแสดงตามสมการต่อไปนี้

$$\text{ความกว้างของอันตรภาคชั้น} = \frac{\text{ข้อมูลที่มีค่าสูงสุด} - \text{ข้อมูลที่มีค่าต่ำสุด}}{\text{จำนวนชั้น}}$$

$$= \frac{5 - 1}{5}$$

$$= 0.8$$

จากหลักเกณฑ์ดังกล่าว สามารถแปลความหมายของค่าคะแนนได้ดังตารางที่ 3.5

ตารางที่ 3.5 เกณฑ์สรุปความเสี่ยง

คะแนน	ระดับความเสี่ยง
4.21 – 5.00	เสี่ยงมากที่สุด
3.41 – 4.20	เสี่ยงมาก
2.61 – 3.40	เสี่ยงปานกลาง
1.81 – 2.60	เสี่ยงน้อย
1.00 – 1.80	เสี่ยงน้อยที่สุด

ตอนที่ 3 เป็นแบบสอบถามความคิดเห็นและข้อเสนอแนะเพิ่มเติม

3.3.4 การตรวจสอบคุณภาพของเครื่องมือ

ในการศึกษาวิจัย ผู้วิจัยได้ทำการทดสอบความเที่ยงตรง (Validity) และความเชื่อมั่น (Reliability) ดังนี้

3.3.1.1 การทดสอบความเที่ยงตรงของเนื้อหา (Content Validity)

ผู้วิจัยนำแบบสอบถามที่สร้างเสร็จแล้วให้อาจารย์ที่ปรึกษาวิทยานิพนธ์ และผู้ทรงคุณวุฒิในฐานะผู้เชี่ยวชาญที่มีความเกี่ยวข้องจำนวน 3 ท่าน ซึ่งแสดงดังภาคผนวก ข เพื่อตรวจสอบความถูกต้องของเนื้อหา ประเมินความสอดคล้องระหว่างข้อคำถามกับนิยามศัพท์ พร้อมทั้งนำผลคะแนนของผู้ทรงคุณวุฒิทั้ง 3 ท่าน มาทำการตรวจสอบความเที่ยงตรงเชิงเนื้อหา (Content Validity) (พรรณี ลีกิจวัฒนะ, 2559) ซึ่งแสดงดังตารางที่ 3.6

ตารางที่ 3.6 เกณฑ์ประเมินความสอดคล้อง

คะแนน	ระดับความสอดคล้อง
$+1$	สอดคล้องกับนิยามศัพท์ที่กำหนดให้
0	ไม่แน่ใจว่าสอดคล้องกับนิยามศัพท์ที่กำหนดให้
-1	ไม่สอดคล้องกับนิยามศัพท์ที่กำหนดให้

จากนั้นนำผลที่ได้ไปหาค่าดัชนีความสอดคล้อง (IOC: Index of Congruency) (พรรณี ลีกิจวัฒนะ, 2559) ซึ่งมีสูตรในการคำนวณดังสมการต่อไปนี้

$$\mathrm{IOC} = \frac{\Sigma \mathrm{R}}{\mathrm{N}}$$

เมื่อ IOC แทน ดัชนีความสอดคล้อง

R แทน ค่าคะแนนรายข้อตามดุลยพินิจของผู้ทรงคุณวุฒิ

Σ แทน ผลรวม

N แทน จำนวนผู้ทรงคุณวุฒิ

ทั้งนี้ ค่า IOC ที่ได้ต้องมากกว่าหรือเท่ากับ 0.5 ขึ้นไป ($IOC \geq 0.5$) ซึ่งคำนวณค่าดัชนีความสอดคล้อง (IOC) ได้ค่าอยู่ระหว่าง 0.67 – 1 ในทุกข้อคำถาม ซึ่งผ่านเกณฑ์ ดังนั้นแบบสอบถามที่จัดทำขึ้น จึงเหมาะสมที่จะนำไปใช้งานต่อไป

3.3.1.2 การทดสอบความเชื่อมั่น (Reliability)

ผู้วิจัยทำการวัดความเชื่อมั่นหรือความสอดคล้องภายในด้วยค่าสัมประสิทธิ์แอลฟาของครอนบาค (Cronbach's alpha coefficient) ด้วยการนำแบบสอบถามที่ได้ดำเนินการปรับปรุงตามคำแนะนำของผู้ทรงคุณวุฒิไปให้กลุ่มตัวอย่างที่มีลักษณะใกล้เคียงกับกลุ่มตัวอย่างในงานวิจัย จำนวน 30 คน โดยมีสูตรในการคำนวณดังสมการต่อไปนี้ (พรรณี ลีกิจวัฒนะ, 2559)

$$\alpha = \frac{n}{n-1}\left[1 - \frac{\sum_i V_i}{V_t}\right]$$

เมื่อ α แทน ความเชื่อมั่นของเครื่องมือ

n แทน จำนวนข้อ

V_i แทน ความแปรปรวนของคะแนนแต่ละข้อ

V_t แทน ความแปรปรวนของคะแนนรวมทุกข้อ

ผลการตรวจสอบความเชื่อมั่น (Reliability) ของเครื่องมือในแต่ละตัวแปรมีค่าความเชื่อมั่นมากกว่า 0.7 ดังนั้นแบบสอบถามที่จัดทำขึ้น จึงเหมาะสมที่จะนำไปใช้งานต่อไป

หลังจากนั้นจะปรับปรุงแบบสอบถามให้สมบูรณ์ โดยตรวจสอบรูปแบบ บรรทัดการพิมพ์ หลักภาษา และนำแบบสอบถามปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัลไปให้อาจารย์ที่ปรึกษาวิทยานิพนธ์ตรวจสอบอีกครั้งหนึ่ง เพื่อเตรียมการจัดพิมพ์แบบสมบูรณ์ ในเวอร์ชั่นปกติและเวอร์ชั่นออนไลน์ผ่าน Google Forms

3.4 วิธีการเก็บรวบรวมข้อมูล

การเก็บรวบรวมข้อมูล ผู้วิจัยได้เก็บข้อมูลโดยดำเนินการตามลำดับขั้นตอนต่อไปนี้

ขั้นที่ 1 ขอความร่วมมือจากผู้ตอบแบบสอบถาม โดยผู้วิจัยอธิบายขั้นตอนและชี้แจงรายละเอียดเกี่ยวกับวัตถุประสงค์ของแบบสอบถาม วิธีเก็บข้อมูล โดยการเก็บข้อมูลตั้งแต่ปลายเดือนธันวาคม พ.ศ. 2563 ถึงพฤษภาคม พ.ศ. 2564 เป็นระยะเวลาประมาณ 6 เดือน

ขั้นที่ 2 ผู้วิจัยตรวจดูความสมบูรณ์ของแบบสอบถามในแต่ละข้อ นับจำนวนแบบสอบถามให้ครบตามจำนวนที่ต้องการ หากพบว่าแบบสอบถามชุดใดผู้ตอบแบบสอบถามทำไม่สมบูรณ์ ผู้วิจัยจะดำเนินการเก็บแบบสอบถามเพิ่มเติมเพื่อให้ได้ข้อมูลครบ 1,067 ชุด จากนั้นนำข้อมูลแบบสอบถามไปวิเคราะห์ตามวิธีทางสถิติและสร้างแบบจำลองต่อไป

3.5 สถิติที่ใช้และการพัฒนาแบบจำลอง

3.5.1 สถิติที่ใช้

สถิติที่ใช้ในการวิเคราะห์ข้อมูลในการวิจัย เรื่อง “การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล” มีดังนี้

1. ค่าเฉลี่ยเลขคณิต (Mean) ใช้สูตร

$$\bar{x} = \frac{\Sigma x}{N}$$

เมื่อ $\bar{x}$ แทน ค่าเฉลี่ย

Σ แทน ผลรวม

x แทน ข้อมูลแต่ละจำนวน

N แทน จำนวนข้อมูลทั้งหมด

3.5.2 การพัฒนาแบบจำลอง

การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล พัฒนาขึ้นโดยใช้กรอบแนวคิดการพัฒนาแบบจำลองด้วยเทคนิคเหมืองข้อมูล (Shu, 2020) ซึ่งประกอบด้วย 7 ขั้นตอน ได้แก่

3.5.2.1 การกรองข้อมูล (Data Cleaning) ผู้วิจัยได้ดำเนินการดาวน์โหลดข้อมูลจาก Google Forms ออกมาเป็นไฟล์รูปแบบ XLSX เพื่อความง่ายต่อการตรวจสอบคุณลักษณะของข้อมูล ตรวจสอบอักขระพิเศษ ตัดคอลัมน์ที่ไม่จำเป็นออก ตัดคอลัมน์ที่มีค่าว่าง และแปลงข้อมูลเป็นภาษาอังกฤษ

3.5.2.2 การรวมข้อมูล (Data Integration) ผู้วิจัยได้ดำเนินการรวมข้อมูลจาก Google Forms และข้อมูลในรูปแบบกระดาษ เป็นข้อมูลชุดเดียวกัน โดยเพิ่มข้อมูลในรูปแบบกระดาษไปรวมกับข้อมูลใน Google Forms ที่ดาวน์โหลดออกมาเป็นไฟล์รูปแบบ XLSX และคำนวณผลลัพธ์ตามเกณฑ์ความเสี่ยงไว้ในคอลัมน์สุดท้าย

3.5.2.3 การคัดเลือกข้อมูล (Data Selection) ผู้วิจัยได้ดำเนินการคัดเลือกข้อมูลที่ผู้ตอบได้กลั่นกรองข้อคำถามตามความจริงทุกข้อ ซึ่งมีข้อคำถามที่ (3.3), (5.3) และ (5.4) ที่มีทิศทางตรงข้ามกับข้ออื่น ๆ ผู้วิจัยจึงสามารถตรวจสอบการตอบคำถามของผู้ตอบได้

3.5.2.4 การแปลงรูปแบบข้อมูล (Data Transformation) ผู้วิจัยได้ดำเนินการแปลงข้อมูลทั้งหมดเป็นรูปแบบที่สามารถอ่านแล้วเข้าใจได้ โดยแปลงเกณฑ์แบบสอบถามปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัลจากคะแนนเป็นข้อความระดับความจริง และผู้วิจัยได้ดำเนินการแปลงไฟล์รูปแบบ XLSX เป็นไฟล์รูปแบบ CSV เพื่อจัดเตรียมข้อมูลเข้าซอฟต์แวร์เวกา (Waikato Environment for Knowledge Analysis: WEKA)

3.5.2.5 การค้นหาแบบจำลอง (Data Mining) ผู้วิจัยได้นำข้อมูลที่สมบูรณ์แล้วเข้าซอฟต์แวร์เวกา (Waikato Environment for Knowledge Analysis: WEKA) โดยคัดเลือกเทคนิคต้นไม้ตัดสินใจ (Decision tree) นาอีฟเบย์ (Naive Baye) และซัพพอร์ตเวกเตอร์แมชชีน (Support Vector Machine)

3.5.2.6 การประเมินแบบจำลอง (Pattern Evaluation) ผู้วิจัยได้ประเมินจากค่าประสิทธิภาพ โดยเปรียบเทียบเทคนิคจำแนกข้อมูลและวิธีการสร้างแบบจำลองที่ให้ค่าความถูกต้อง (Accuracy) สูงที่สุด

3.5.2.7 การนำเสนอความรู้ที่ค้นพบ (Knowledge Representation) ผู้วิจัยนำแบบจำลองที่ได้จากการจำแนกความปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัลมาเขียนองค์ความรู้ในรูปแบบกฎ (Rule)

บทที่ 4

ผลการวิจัย

การวิจัยครั้งนี้มีวัตถุประสงค์ เพื่อศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล และเพื่อพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล โดยวิเคราะห์ด้วยหลักการทางสถิติพร้อมทั้งเสนอผลการวิเคราะห์ข้อมูลในรูปตารางและอธิบายความเรียงโดยแบ่งการนำเสนอออกเป็น 2 ส่วนดังนี้

4.1 ผลการศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

4.2 ผลการพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล

4.1 ผลการศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

ผลการศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล ผู้วิจัยได้ทำการสังเคราะห์ข้อมูลจากเอกสาร (Documentary Research) เพื่อหาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล โดยสามารถสรุปผลปัจจัยการสื่อสารที่ได้ศึกษาตามการอ้างอิงจากผู้ที่กล่าวถึงปัจจัยต่าง ๆ ประกอบด้วย 9 ปัจจัย ซึ่งแสดงดังตารางที่ 4.1

ตารางที่ 4.1 ปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

ลำดับ	ทฤษฎี / งานวิจัยที่เกี่ยวข้อง	(ก) อ้างเป็นบุคคลสำคัญ	(ข) การสร้างความน่าเชื่อถือ	(ค) กระตุ้นความสนใจ	(ง) กระตุ้นความต้องการ	(จ) สร้างความคาดหวัง	(ฉ) ความกลัว	(ช) ความโลภ	(ซ) ความอยากรู้อยากเห็น	(ฌ) การตัดสินใจอย่างไม่มีเหตุผล
1	Information Gap Theory (1994)								✓	✓
2	Ahmed & Omotunde (2012)									✓
3	Ainslie (1975)									✓
4	Birkett (2017)						✓	✓		
5	Breda & Berlamont (2014)						✓	✓		✓
6	Dijkstra (2018)							✓	✓	✓
7	Golman & Loewenstein (2015)						✓		✓	
8	Hooper & Blunt (2020)			✓			✓			
9	House & Raja (2020)				✓		✓			
10	Jansen & van Schaik (2019)						✓		✓	
11	Musuva, Getao & Chepken (2019)			✓						✓
12	Albladi & George (2017)		✓						✓	✓

ตารางที่ 4.1 ปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล (ต่อ)

ลำดับ	ทฤษฎี / งานวิจัยที่เกี่ยวข้อง	(ก) อ้างเป็นบุคคลสำคัญ	(ข) การสร้างความน่าเชื่อถือ	(ค) กระตุ้นความสนใจ	(ง) กระตุ้นความต้องการ	(จ) สร้างความคาดหวัง	(ฉ) ความกลัว	(ช) ความโลภ	(ซ) ความอยากรู้อยากเห็น	(ฌ) การตัดสินใจอย่างไม่มีเหตุผล
13	Jansen, J. & Van Schaik (2018)		✓			✓				
14	Sharp & Wu (2017)	✓			✓	✓				
15	Wang & Rao (2017)							✓	✓	✓
16	ArachcilageLove & Benznosov (2016)	✓	✓							
17	Harrison, Svetieva & Vishwanath (2016)			✓	✓	✓				
18	Alseadoon, Ibrahim & Oihman (2015)	✓	✓							
19	Halevi, Memon & Nov (2015)	✓	✓			✓				
20	Harrison, Vishwanath & Rao (2015)			✓	✓					
21	Reyns (2015)	✓				✓				
22	Leukfeldt & Yar (2014)	✓	✓		✓	✓				
23	Purkait (2014)			✓	✓					✓

ตารางที่ 4.1 ปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล (ต่อ)

ลำดับ	ทฤษฎี / งานวิจัยที่เกี่ยวข้อง	(ก) อ้างเป็นบุคคลสำคัญ	(ข) การสร้างความน่าเชื่อถือ	(ค) กระตุ้นความสนใจ	(ง) กระตุ้นความต้องการ	(จ) สร้างความคาดหวัง	(ฉ) ความกลัว	(ช) ความโลภ	(ซ) ความอยากรู้อยากเห็น	(ฌ) การตัดสินใจอย่างไม่มีเหตุผล
24	Luo, Zhang, Burd & Seazzu (2013)									✓
25	Yoon & Kim (2013)		✓						✓	
26	Pattinson, Jerram, Parsons, Mccormac & Butavicius (2012)				✓				✓	
27	Wang (2012)	✓	✓	✓	✓	✓				
28	Ngo & Paternoster (2011)								✓	✓
29	Vishwanath, Herath, Chen, Wang, & Rao (2011)		✓	✓	✓	✓				
30	Parrish, Bailey & Courtney (2015)	✓								
31	Sheng, Holbrook, Kumaraguru, Cranor & Downs (2010)	✓	✓							
32	Wright & Marett (2010)	✓	✓							

ตารางที่ 4.1 ปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล (ต่อ)

ลำดับ	ทฤษฎี / งานวิจัยที่เกี่ยวข้อง	(ก) อ้างเป็นบุคคลสำคัญ	(ข) การสร้างความน่าเชื่อถือ	(ค) กระตุ้นความสนใจ	(ง) กระตุ้นความต้องการ	(จ) สร้างความคาดหวัง	(ฉ) ความกลัว	(ช) ความโลภ	(ซ) ความอยากรู้อยากเห็น	(ฌ) การตัดสินใจอย่างไม่มีเหตุผล
33	Hill, Fombelle & Sirianni (2016)			✓	✓	✓		✓	✓	✓
34	Kahneman (2011)									✓
35	Laran & Tsiros (2013)			✓	✓					✓
36	Litman & Spielberger (2003)						✓		✓	
37	Mussel et al. (2015)							✓	✓	✓
38	Sakaki, Yagi & Murayama (2018)						✓		✓	
39	Seuntjens et al. (2015)							✓	✓	✓
40	Spielberger (2004)							✓		
41	Limandri (1998)						✓			
42	ชานนท์ สำเภาอินทร์ (2557)						✓			
43	เบญจพร ลิ้มธรรมาภรณ์ (2554)	✓				✓				
44	สุรชัย ฉัตรเฉลิมพันธุ์ (2563)	✓	✓							
45	ปวันตา บุญพันธ์ (2557)						✓			

ตารางที่ 4.1 ปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล (ต่อ)

ลำดับ	ทฤษฎี / งานวิจัยที่เกี่ยวข้อง	(ก) อ้างเป็นบุคคลสำคัญ	(ข) การสร้างความน่าเชื่อถือ	(ค) กระตุ้นความสนใจ	(ง) กระตุ้นความต้องการ	(จ) สร้างความคาดหวัง	(ฉ) ความกลัว	(ช) ความโลภ	(ซ) ความอยากรู้อยากเห็น	(ฌ) การตัดสินใจอย่างไม่มีเหตุผล
46	สุดารัตน์ วงศ์คำ (2550)							✓		
47	ฐิติมา อินกล่ำ (2558)	✓	✓		✓	✓		✓		✓
48	ตฤณ ทวิธารานนท์ (2562)			✓	✓	✓				
49	สุนันทา เรียงแหลม (2551)							✓		
50	พงศ์พนธ์ ภาวศุทธิ์ (2561)						✓	✓	✓	✓

จากตารางที่ 4.1 พบว่าปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล ประกอบไปด้วย 9 ปัจจัย ได้แก่ อ้างเป็นบุคคลสำคัญ การสร้างความน่าเชื่อถือ กระตุ้นความสนใจ กระตุ้นความต้องการ สร้างความคาดหวัง ความกลัว ความโลภ ความอยากรู้อยากเห็น และการตัดสินใจอย่างไม่มีเหตุผล ซึ่งผู้วิจัยได้นำปัจจัยเหล่านี้ไปพัฒนาแบบวัด

4.2 ผลการพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล

การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล ผู้วิจัยได้เริ่มต้นขั้นตอนการพัฒนาแบบจำลองจากการคัดเลือกเทคนิคจำแนกข้อมูลที่ให้ค่าความถูกต้องที่สุด โดยได้คัดเลือกเทคนิคต้นไม้ตัดสินใจ (Decision

Tree : J48) เทคนิคนาอีฟเบย์ (Naïve Bayes) และเทคนิคซัพพอร์ตเวกเตอร์แมชชีน (Support Vector Machaine) รวมทั้งหมด 3 เทคนิค แสดงค่าความถูกต้องดังตารางที่ 4.2

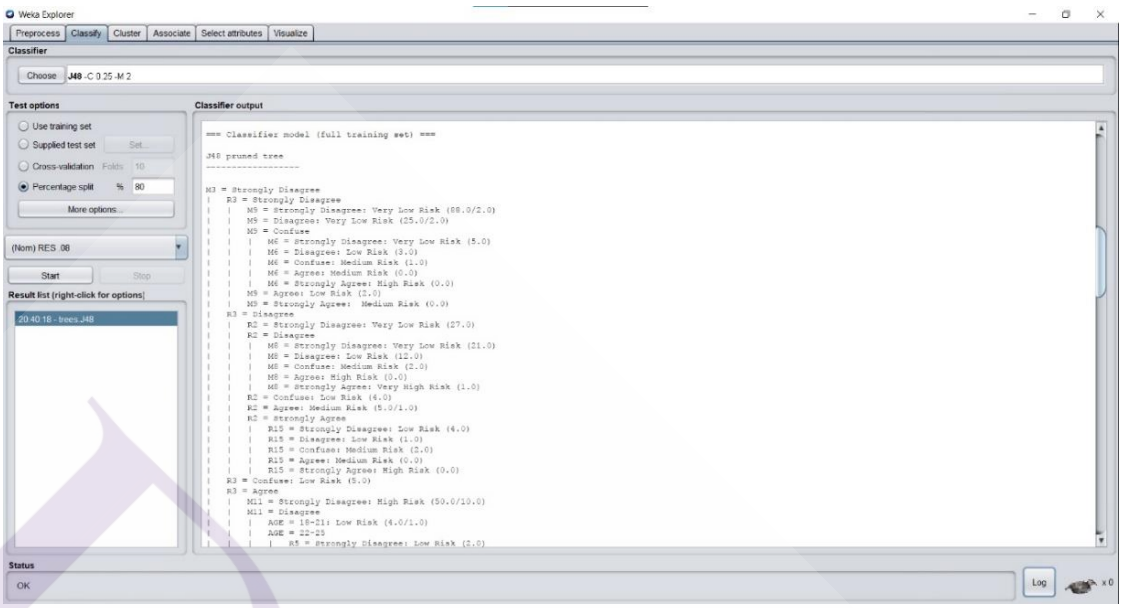
ตารางที่ 4.2 ค่าความถูกต้อง (Accuracy) ของแบบจำลองจากการทดสอบด้วยเทคนิคต่าง ๆ

วิธีสร้างแบบจำลอง	ค่าความถูกต้องจากการทดสอบด้วยเทคนิคต่าง ๆ		
	เทคนิค ต้นไม้ตัดสินใจ J48	เทคนิค นาอีฟเบย์	เทคนิคซัพพอร์ต เวกเตอร์แมชชีน
การตรวจสอบไขว้ (5-fold)	89.61	89.46	87.62
การตรวจสอบไขว้ (10-fold)	87.54	88.02	88.14
การตรวจสอบไขว้ (20-fold)	93.41	89.01	90.34
การแบ่งข้อมูลแบบสุ่มด้วยการแบ่งร้อยละ 20	91.23	86.06	87.52
การแบ่งข้อมูลแบบสุ่มด้วยการแบ่งร้อยละ 66	93.12	88.88	91.06
การแบ่งข้อมูลแบบสุ่มด้วยการแบ่งร้อยละ 80	94.57	86.48	93.04
การแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน (80:20)	95.49	87.14	92.13
ค่าเฉลี่ย	**92.13**	**87.86**	**89.97**

จากตารางที่ 4.2 พบว่าการสร้างแบบจำลองโดยใช้เทคนิคต้นไม้ตัดสินใจ (Decision Tree : J48) มีค่าเฉลี่ยความถูกต้อง (Accuracy) สูงกว่าเทคนิคอื่น โดยมีค่าเฉลี่ยความถูกต้องเท่ากับ 92.13 รองลงมาเป็นเทคนิคซัพพอร์ตเวกเตอร์แมชชีนมีค่าเฉลี่ยความถูกต้องเท่ากับ 89.97 โดยเทคนิคนาอีฟเบย์มีค่าเฉลี่ยความถูกต้องน้อยที่สุด คิดเป็นร้อยละ 87.86

จากนั้นผู้วิจัยใช้โปรแกรม Weka สร้างและทดสอบตัวแบบ พบว่าเทคนิคต้นไม้ตัดสินใจ (J48) โดยใช้วิธีการแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน (Training set and test set) 80:20 มีความถูกต้องมากที่สุด และผลลัพธ์ที่ได้จากต้นไม้ตัดสินใจ J48 มีลักษณะดังแสดงในภาพที่ 4.1 โดยได้กฎทั้งสิ้นจำนวน 118 กฎ (กฎที่ได้จากการวิเคราะห์ด้วยต้นไม้ตัดสินใจ J48 แสดงในภาคผนวก ช. หน้า 148) เมื่อนำต้นไม้ตัดสินใจ J48 แสดงดังภาพที่ 4.2 มาเขียนเป็นกฎด้วยเงื่อนไข IF…Then… แสดงดังตารางที่ 4.3

ภาพ 4.1 ต้นไม้ตัดสินใจที่ได้



ภาพ 4.2 ส่วนของแบบจำลองที่ได้จากการใช้เทคนิคจำแนกข้อมูลแบบ J48

ตารางที่ 4.3 ตัวอย่างกฎที่ได้จากการวิเคราะห์ด้วยต้นไม้ตัดสินใจ J48

ลำดับที่	กฎที่ได้จากต้นไม้ตัดสินใจ J48	ความเสี่ยงต่อการถูกล่อลวง
1	M3 = Strongly Disagree R3 = Strongly Disagree M9 = Strongly Disagree	Very Low Risk
2	M3 = Strongly Disagree R3 = Strongly Disagree M9 = Disagree	Very Low Risk
3	M3 = Strongly Disagree R3 = Strongly Disagree M9 = Confuse M6 = Strongly Disagree	Very Low Risk
4	M3 = Strongly Disagree R3 = Strongly Disagree M9 = Confuse M6 = Disagree	Low Risk
5	M3 = Strongly Disagree R3 = Strongly Disagree M9 = Confuse M6 = Confuse	Medium Risk

ตารางที่ 4.3 ตัวอย่างกฎที่ได้จากการวิเคราะห์ด้วยต้นไม้ตัดสินใจ J48 (ต่อ)

ลำดับที่	กฎที่ได้จากต้นไม้ตัดสินใจ J48		ความเสี่ยงต่อการถูกล่อลวง
6	M3 = Strongly Disagree M9 = Confuse	R3 = Strongly Disagree M6 = Agree	Medium Risk
7	M3 = Strongly Disagree M9 = Confuse	R3 = Strongly Disagree M6 = Strongly Agree	High Risk
8	M3 = Strongly Disagree M9 = Agree	R3 = Strongly Disagree	Low Risk
9	M3 = Strongly Disagree M9 = Strongly Agree	R3 = Strongly Disagree	Medium Risk
10	M3 = Strongly Disagree R2 = Strongly Disagree	R3 = Disagree	Very Low Risk

จากตารางที่ 4.3 ซึ่งเป็นกฎที่ได้จากการวิเคราะห์ด้วยต้นไม้ตัดสินใจ J48 สามารถแปรผลความเสี่ยงต่อการถูกล่อลวงได้ดังเช่น กฎลำดับที่ 1 ไม่เห็นด้วยที่สุดกับข้อความ “ท่านจะไม่ส่งต่อข้อมูลเหล่านั้น หากพบว่าเป็นข่าวปลอม แชร์ลูกโซ่” ไม่เห็นด้วยที่สุดกับข้อความ “ท่านรู้สึกกลัวเมื่อมีผู้อ้างว่าครอบครองภาพลับของท่านไว้” และ ไม่เห็นด้วยที่สุดกับข้อความ “ท่านรู้สึกดีใจหากได้รับข้อความว่าได้รับเงินช่วยเหลือสวัสดิการจากภาครัฐ” จะมีความเสี่ยงต่อการถูกล่อลวงอยู่ในระดับเสี่ยงน้อยที่สุด หรือ กฎลำดับที่ 7 ไม่เห็นด้วยที่สุดกับข้อความ “ท่านจะไม่ส่งต่อข้อมูลเหล่านั้น หากพบว่าเป็นข่าวปลอม แชร์ลูกโซ่” ไม่เห็นด้วยที่สุดกับข้อความ “ท่านรู้สึกกลัว เมื่อมีผู้อ้างว่าครอบครองภาพลับของท่านไว้” ไม่แน่ใจกับข้อความ “ท่านรู้สึกดีใจหากได้รับข้อความว่าได้รับเงินช่วยเหลือสวัสดิการจากภาครัฐ” แต่ท่านเห็นด้วยที่สุดกับข้อความ “ท่านยินดีบอกข้อมูลให้กับทนายอาสาบนโลกออนไลน์ที่บอกว่าจะช่วยให้ท่านไม่ถูกดำเนินคดี” จะมีความเสี่ยงต่อการถูกล่อลวงอยู่ในระดับเสี่ยงมากที่สุด

บทที่ 5

สรุปผล อภิปราย และข้อเสนอแนะ

การวิจัยเรื่อง “การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล” มีวัตถุประสงค์การวิจัยดังนี้

1. เพื่อศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล
2. เพื่อพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล

ผู้วิจัยได้นำทฤษฎี แนวคิด และผลงานวิจัยที่เกี่ยวข้องมาศึกษาและเป็นกรอบแนวคิดในการวิเคราะห์ ประกอบไปด้วย ทฤษฎีการสื่อสารยุคดิจิทัล ทฤษฎีและแนวคิดเกี่ยวกับดิจิทัล การถูกล่อลวงบนสื่อดิจิทัล เทคนิคเหมืองข้อมูล และต้นไม้ตัดสินใจ

ใช้วิธีการวิจัยและพัฒนา (Research and Development) ทำการเก็บรวบรวมข้อมูลกลุ่มตัวอย่าง ผู้รับสารกลุ่มดิจิทัลเนทีฟ จำนวน 1,067 คน เมื่อเก็บรวบรวมข้อมูลครบตามที่กำหนดแล้ว จึงนำมาดำเนินการทางสถิติเพื่อการวิเคราะห์ข้อมูล

จากนั้นนำปัจจัยที่ได้จากการศึกษาในขั้นตอนแรก และข้อมูลที่รวบรวมได้จากกลุ่มตัวอย่าง มาพัฒนาเป็นแบบจำลอง โดยทดสอบด้วยเทคนิคต่าง ๆ และคัดเลือกเทคนิคที่มีค่าความถูกต้อง (Accuracy) สูงที่สุด

โดยสามารถสรุปผลการดำเนินงานและข้อเสนอแนะ โดยแบ่งเป็น 3 หัวข้อ ดังนี้

5.1 สรุปผลการวิจัย

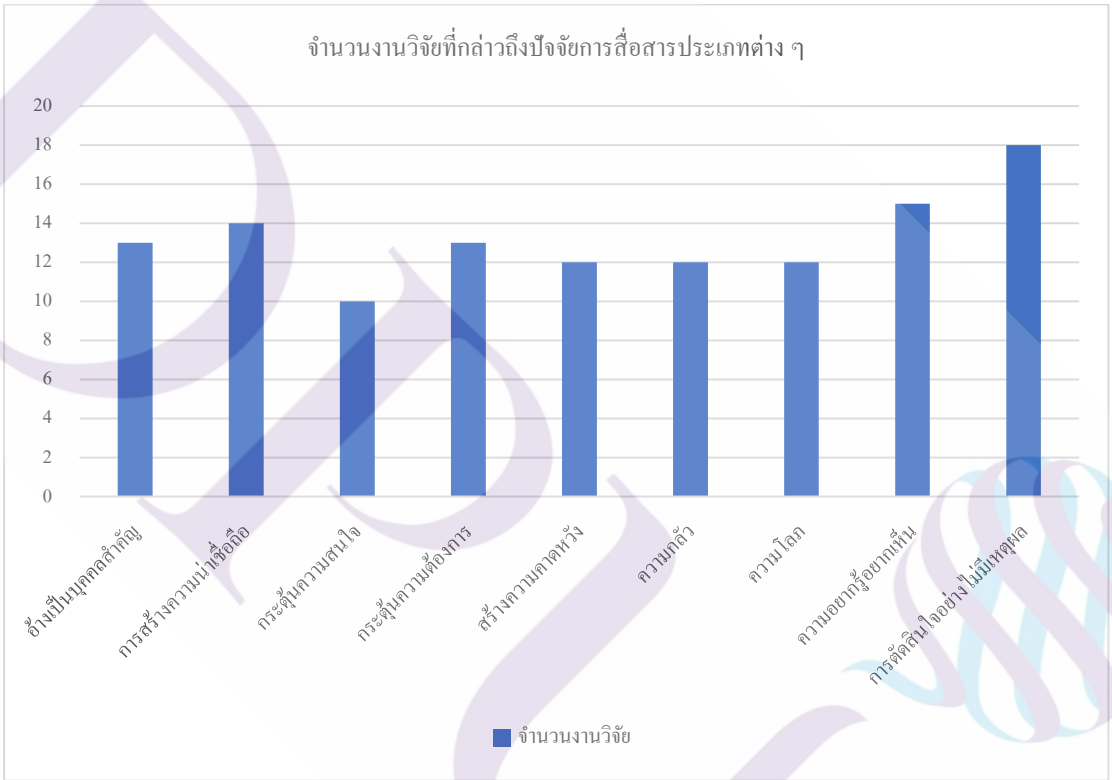
5.2 การอภิปรายผลการวิจัย

5.3 ข้อเสนอแนะเพื่อการวิจัย

5.1 สรุปผลการวิจัย

การดำเนินการที่กล่าวมาข้างต้น ผู้วิจัยได้นำข้อมูลที่ได้มาสรุปผลการวิจัย ดังนี้

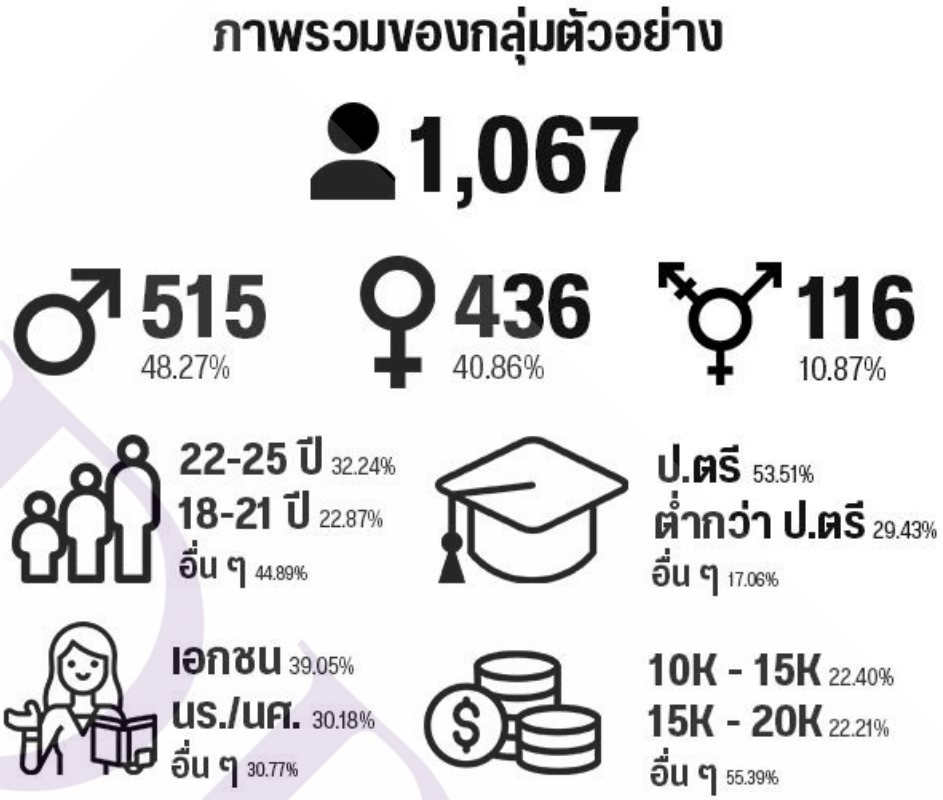
5.1.1 การศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล ผู้วิจัยได้นำทฤษฎี แนวคิด และผลงานวิจัยที่เกี่ยวข้องมาศึกษา โดยได้ปัจจัยที่เกี่ยวข้องกับการสื่อสาร จำนวน 9 ปัจจัย ได้แก่ อ้างเป็นบุคคลสำคัญ การสร้างความน่าเชื่อถือ กระตุ้นความสนใจ กระตุ้นความต้องการ สร้างความคาดหวัง ความกลัว ความโลภ ความอยากรู้อยากเห็น และการตัดสินใจอย่างไม่มีเหตุผล



ภาพที่ 5.1 แสดงจำนวนงานวิจัยที่กล่าวถึงปัจจัยการสื่อสารประเภทต่าง ๆ

จากภาพที่ 5.1 แสดงจำนวนงานวิจัยที่กล่าวถึงปัจจัยการสื่อสารประเภทต่าง ๆ พบว่า ปัจจัยด้านความโลภ และปัจจัยด้านการตัดสินใจอย่างไม่มีเหตุผล มีงานวิจัยกล่าวถึงมากที่สุดถึง 18 วิจัย ส่วนปัจจัยด้านอื่น ๆ มีจำนวนงานที่กล่าวถึงใกล้เคียงกัน

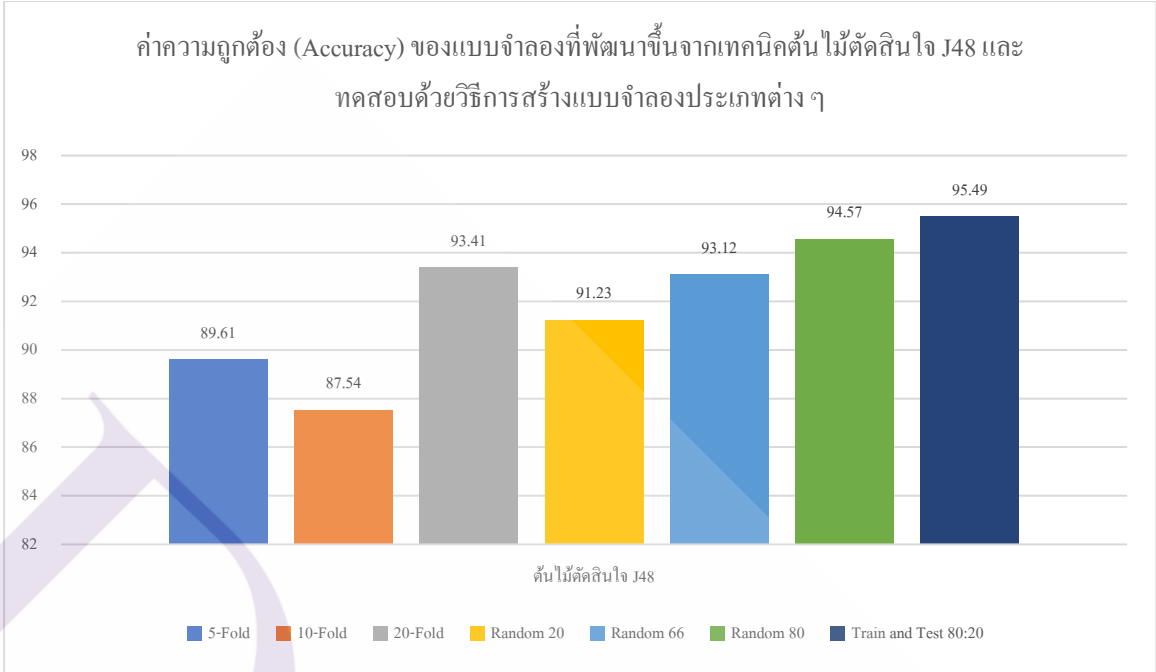
จากนั้นนำปัจจัยที่ได้มาดำเนินการจัดทำแบบสอบถาม โดยเก็บรวบรวมข้อมูลตั้งแต่ เดือนธันวาคม พ.ศ. 2563 ถึงเดือนพฤษภาคม พ.ศ. 2564 จำนวน รวมทั้งสิ้น 1,067 กลุ่มตัวอย่าง และนำข้อมูลดังกล่าวมาวิเคราะห์



ภาพที่ 5.2 แสดงภาพรวมของกลุ่มตัวอย่าง

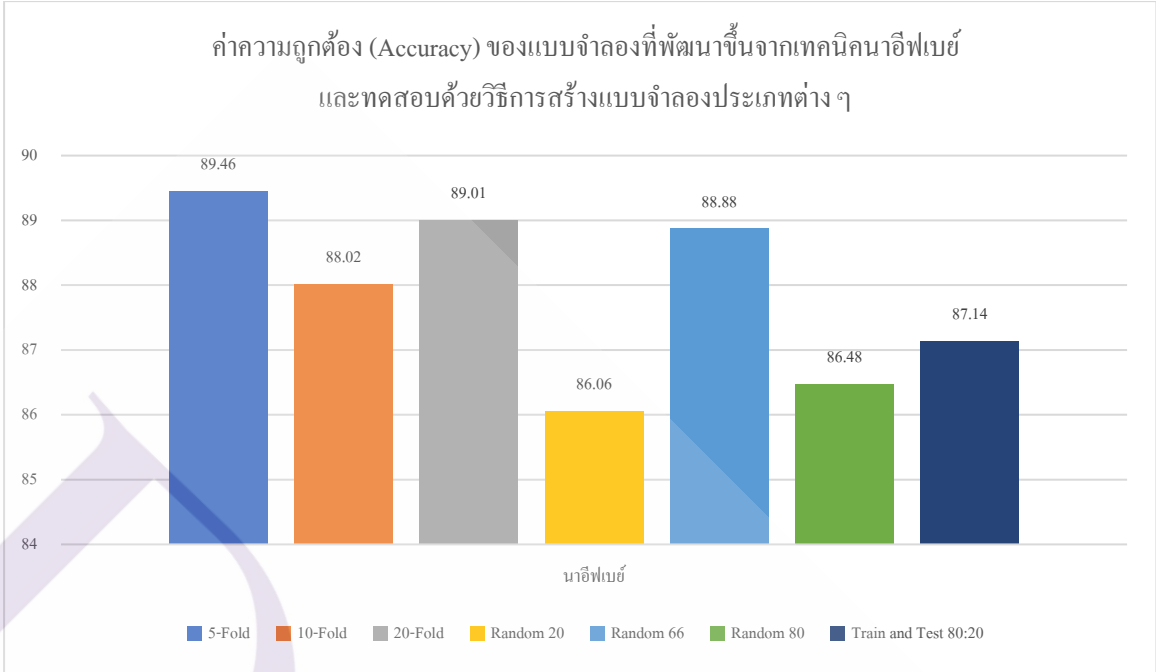
จากภาพที่ 5.2 จะเห็นว่า กลุ่มตัวอย่างที่ทำการศึกษามีทั้งสิ้น 1,067 คน กลุ่มตัวอย่างส่วนใหญ่เป็นเพศชาย คิดเป็นร้อยละ 48.27 มีอายุระหว่าง 22-25 ปี คิดเป็นร้อยละ 32.24 จบการศึกษาระดับปริญญาตรีคิดเป็นร้อยละ 53.51 ประกอบอาชีพพนักงานบริษัทเอกชนคิดเป็นร้อยละ 39.95 และมีรายได้อยู่ระหว่าง 10,000 ถึง 15,000 บาท คิดเป็นร้อยละ 22.40

5.1.2 การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล ผู้วิจัยดำเนินการพัฒนาแบบจำลองจากการคัดเลือกเทคนิคจำแนกข้อมูลที่ให้ค่าความถูกต้อง (Accuracy) สูงที่สุด โดยได้คัดเลือกเทคนิคต้นไม้ตัดสินใจ (Decision Tree : J48) เทคนิคนาอีฟเบย์ (Naïve Bayes) และเทคนิคซัพพอร์ตเวกเตอร์แมชชีน (Support Vector Machaine) รวมทั้งหมด 3 เทคนิค จากนั้นทำการพัฒนาตัวแบบจำลองโดยแบ่งออกเป็น 3 วิธี คือ การตรวจสอบไขว้ การแบ่งข้อมูลแบบสุ่มด้วยการแบ่งร้อยละ และการแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน



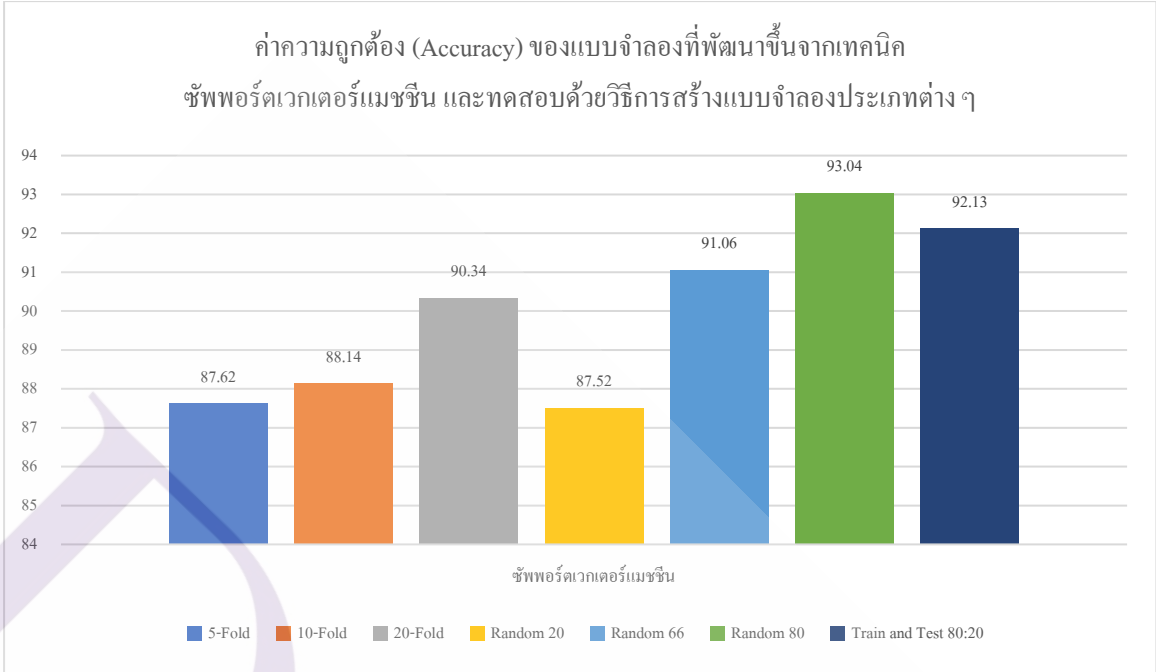
ภาพที่ 5.3 แสดงการเปรียบเทียบค่าความถูกต้อง (Accuracy) ของแบบจำลองที่พัฒนาขึ้นจากเทคนิคต้นไม้ตัดสินใจ J48 และทดสอบด้วยวิธีการสร้างแบบจำลองประเภทต่าง ๆ

จากภาพที่ 5.3 พบว่าเทคนิคต้นไม้ตัดสินใจ ที่สร้างด้วยวิธีการการแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน 80:20 มีค่าความถูกต้อง (Accuracy) สูงที่สุดคิดเป็นร้อยละ 95.49 รองลงมาเป็นวิธีการแบ่งข้อมูลแบบสุ่มด้วยการแบ่งร้อยละ 80 มีค่าความถูกต้องร้อยละ 94.57 โดยวิธีการตรวจสอบไขว้ (10-fold) มีค่าความถูกต้องน้อยที่สุดคิดเป็นร้อยละ 87.54



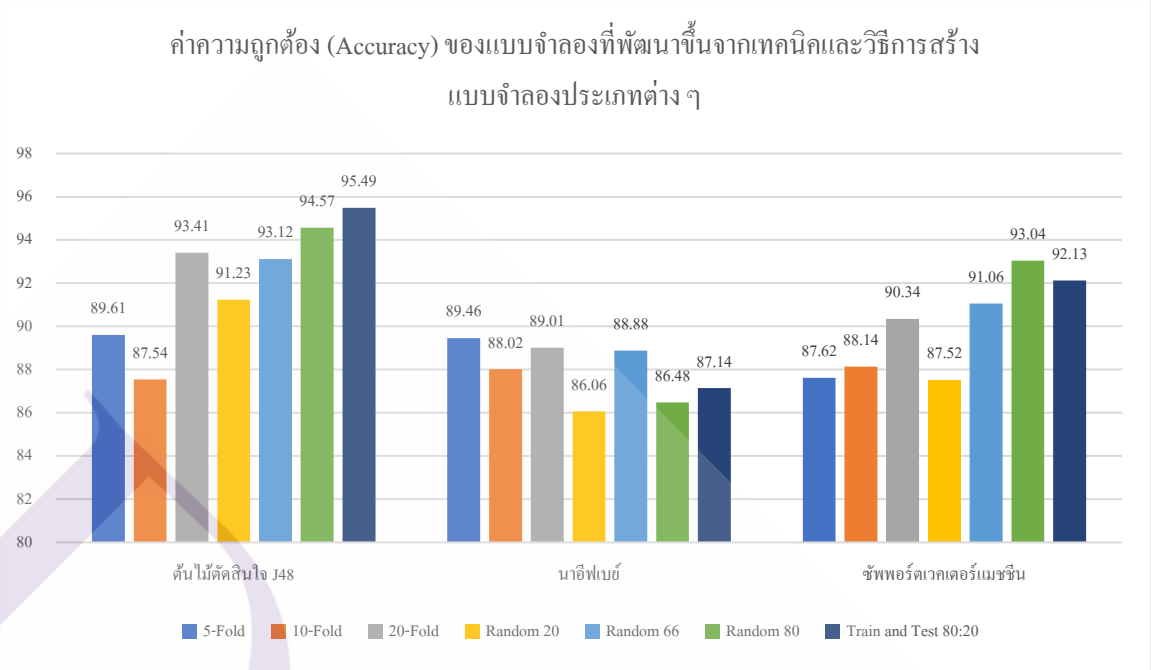
ภาพที่ 5.4 แสดงการเปรียบเทียบค่าความถูกต้อง (Accuracy) ของแบบจำลองที่พัฒนาขึ้นจากเทคนิคนาอีฟเบย์ และทดสอบด้วยวิธีการสร้างแบบจำลองประเภทต่าง ๆ

จากภาพที่ 5.4 พบว่าเทคนิคนาอีฟเบย์ ที่สร้างด้วยวิธีการตรวจสอบไขว้ (10-fold) มีค่าความถูกต้อง (Accuracy) สูงที่สุดคิดเป็นร้อยละ 89.46 รองลงมาเป็นวิธีการตรวจสอบไขว้ (20-fold) มีค่าความถูกต้องร้อยละ 89.01 โดยการแบ่งข้อมูลแบบสุ่มด้วยการแบ่งร้อยละ 20 มีค่าความถูกต้องน้อยที่สุดคิดเป็นร้อยละ 86.06



ภาพที่ 5.5 แสดงการเปรียบเทียบค่าความถูกต้อง (Accuracy) ของแบบจำลองที่พัฒนาขึ้นจากเทคนิคซัพพอร์ตเวกเตอร์แมชชีน และทดสอบด้วยวิธีการสร้างแบบจำลองประเภทต่าง ๆ

จากภาพที่ 5.5 พบว่าเทคนิคซัพพอร์ตเวกเตอร์แมชชีน ที่สร้างด้วยวิธีการแบ่งข้อมูลแบบสุ่มด้วยการแบ่งร้อยละ 80 มีค่าความถูกต้อง (Accuracy) สูงที่สุดคิดเป็นร้อยละ 93.04 รองลงมาเป็นวิธีการแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน 80:20 มีค่าความถูกต้องร้อยละ 92.13 โดยวิธีการแบ่งข้อมูลแบบสุ่มด้วยการแบ่งร้อยละ 20 มีค่าความถูกต้องน้อยที่สุดคิดเป็นร้อยละ 87.52



ภาพที่ 5.6 แสดงการเปรียบเทียบค่าความถูกต้อง (Accuracy) ของแบบจำลองที่พัฒนาขึ้นจากเทคนิคและวิธีการสร้างแบบจำลองประเภทต่าง ๆ

จากภาพที่ 5.6 พบว่าเทคนิคต้นไม้ตัดสินใจ J48 ที่ทำการพัฒนาแบบจำลองโดยใช้วิธีการแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน จะมีค่าความถูกต้องร้อยละ 95.49 ซึ่งมีค่าประสิทธิภาพสูงกว่าเทคนิคและวิธีการอื่น โดยจะได้ตัวแบบจำลองที่มีกฎการจำแนกข้อมูลทั้งสิ้น 118 กฎ แสดงว่า เทคนิคต้นไม้ตัดสินใจ J48 ที่ทำการพัฒนาแบบจำลองโดยใช้วิธีการแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน สามารถนำไปใช้ในการพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัลได้ เนื่องจากเป็นเทคนิคและรูปแบบที่มีความถูกต้องแม่นยำสูงกว่าเทคนิคและวิธีการอื่น

5.2 การอภิปรายผล

จากผลการวิจัยมีประเด็นที่น่าสนใจนำมาอภิปรายผลดังนี้

5.2.1 จากวัตถุประสงค์ที่ว่า “เพื่อศึกษาปัจจัยด้านการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล”

ผู้วิจัยได้กำหนดประเด็นในการศึกษาสำหรับวัตถุประสงค์ข้อนี้ทั้งหมดสองส่วน คือ ส่วนที่เกี่ยวข้องปัจจัยด้านประชากรศาสตร์ ได้แก่ เพศ อายุ การศึกษา อาชีพ และรายได้

และ ส่วนที่เกี่ยวข้องกับปัจจัยด้านการสื่อสาร ผู้วิจัยได้นำทฤษฎีการสื่อสาร Social Media Communication Framework ของ Sasser (2014) ที่กล่าวว่าการสื่อสารมีองค์ประกอบทั้งหมด 4 องค์ประกอบ มาใช้ทั้งหมด 3 องค์ประกอบได้แก่ ผู้ส่งสาร (Sender) สาร (Messages) และผู้รับสาร (Receiver) เนื่องจากการวิจัยครั้งนี้ มุ่งศึกษาเฉพาะการล่อลวงที่เกิดขึ้นบนสื่อดิจิทัลเท่านั้น

5.2.1.1 ผลการศึกษา ปัจจัยทางด้านประชากรศาสตร์ โดยวิเคราะห์ร่วมกับการพัฒนาแบบจำลองด้านการสื่อสาร โดยใช้เทคนิคต้นไม้ตัดสินใจที่สร้างด้วยวิธีการแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน 80:20 พบว่า ปัจจัยทางด้านประชากรศาสตร์ 4 ตัวแปร จากทั้งหมด 5 ตัวแปร ประกอบด้วย เพศ อายุ การศึกษา และอาชีพ มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล ซึ่งสอดคล้องกับ Abroshan (2021) ที่พบว่า ปัจจัยทางประชากรศาสตร์ ทั้ง อายุ เพศ และการศึกษา ส่งผลกระทบโดยตรงหรือโดยอ้อมต่อการถูกล่อลวงด้วยวิธีการฟิชชิ่ง ทั้งเรื่องของการแยกแยะอีเมลสแปม หรือข้อความที่ล่อลวงเป็นต้น สอดคล้องกับ Sheng (2010) ที่พบว่า เพศหญิง มีโอกาสตกเป็นเหยื่อของการโจมตีแบบฟิชชิ่ง มากกว่าเพศอื่น โดยพบพฤติกรรมอันตราย อาทิ การคลิกลิงก์ที่ไม่รู้จักพร้อมทั้งให้ข้อมูลกับเว็บไซต์เหล่านั้น

ในขณะที่ Gratian (2018) พบว่า ระดับการศึกษา มีผลต่อความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล ทั้งนี้ยังพบอีกว่านักศึกษาในคณะบริหารธุรกิจ การศึกษา และศิลปศาสตร์ มีแนวโน้มที่จะถูกโจมตีมากกว่านักศึกษาที่ศึกษาอยู่ในคณะเทคโนโลยี หรือคณะวิทยาศาสตร์ และยังสอดคล้องกับ Williams (2018) ที่พบว่าอาชีพและตำแหน่งหน้าที่ในองค์กรมีผลต่อการถูกล่อลวงบนสื่อดิจิทัลด้วยวิธีฟิชชิ่งที่แตกต่างกัน โดยอาชีพที่ต้องพบปะหรือรับอีเมลจากบุคคลภายนอก เช่น คอลเซ็นเตอร์ ฝ่ายจัดซื้อ มีแนวโน้มที่ได้รับอีเมลฟิชชิ่งมากกว่าอาชีพอื่น เนื่องจากผู้ไม่หวังดีสามารถที่จะเก็บรวบรวมฐานข้อมูลอีเมลเหล่านี้ได้จากแหล่งสาธารณะ

ดังนั้น ผลการค้นพบจากแบบจำลองที่ผู้วิจัยพัฒนาขึ้น เมื่อเปรียบเทียบกับการศึกษาในต่างประเทศ เห็นได้ว่า มีผลการวิจัยไปในทิศทางเดียวกัน คือ องค์ประกอบของตัวแปรทางด้าน

ประชากรศาสตร์ 4 ด้าน ประกอบด้วย เพศ อายุ การศึกษา และอาชีพ มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล ทั้งนี้มีข้อมูลที่สนับสนุนได้ว่า แม้จะเป็นผู้หญิง ที่มีระดับการศึกษาไม่สูง มีอาชีพที่ต้องติดต่อกับบุคคลภายนอก ซึ่งมีแนวโน้มที่จะเสี่ยงต่อการถูกล่อลวงในระดับที่เสี่ยงสูงมาก โดยเฉพาะเพศหญิงที่มีอายุอยู่ในช่วง 18-36 ปี ซึ่งอยู่ในกลุ่มดิจิทัลเนทีฟ (Digital Native) หมายถึง คนที่เกิดมาพร้อมกันกับเทคโนโลยีดิจิทัล แนวคิดทันสมัยตามทันโลก สามารถใช้งานอุปกรณ์ เทคโนโลยี หรือสื่อดิจิทัลได้อย่างคล่องแคล่ว ตามทฤษฎี Digital Native ของ Mac Prensky (2001) หากถูกล่อลวงบนโลกดิจิทัล ไม่ว่าจะเป็นการซื้อสินค้าแล้วไม่ได้รับสินค้า การหลอกโอนเงิน การขอยืมเงินแล้วไม่คืนให้ตามกำหนดเวลา กลุ่มดิจิทัลเนฟทีฟจะมีบทเรียน และภูมิคุ้มกันที่เพิ่มมากขึ้น ทำให้มีโอกาสน้อยมากที่จะถูกหลอกหรือถูกล่อลวงด้วยวิธีการเดิมซ้ำได้อีก

ในขณะผลการวิจัยปรากฏว่า มีเพียงตัวแปรด้านรายได้มีความแตกต่างกับองค์ประกอบทั้ง 4 ด้าน คือ ไม่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล ซึ่งสอดคล้องกับ Griffin (2018) ที่ศึกษาเรื่องการโจมตีด้วยวิธีการฟิชชิ่งพบว่า รายได้ของผู้รับสารไม่ได้มีผลต่อการถูกโจมตี ในขณะที่ปัจจัยด้านอายุ การศึกษา และอาชีพ ส่งผลต่อการโจมตีอย่างมีนัยสำคัญ

อย่างไรก็ตาม สาเหตุที่ตัวแปรด้านรายได้ ไม่ส่งผลกระทบต่อการถูกล่อลวงอาจเกิดจากเงื่อนไขการสร้างแบบจำลอง โดยเมื่อเริ่มทำการสร้างแบบจำลองแล้วตัวโปรแกรม Weka ได้ตัดปัจจัยเกี่ยวกับรายได้ เพราะ ไม่เข้าเงื่อนไขการเลือกแอทริบิว (Attribute selection measure) ซึ่ง โกเมศ อัมพวัน (2553) อธิบายว่า การแบ่งข้อมูลออกเป็นชุดข้อมูลย่อยจะนิยมใช้ค่าเกนความรู้ (Information Gain) ซึ่งจะทำการเลือกแอทริบิวสำหรับแบ่งข้อมูลจากแอทริบิวที่มีค่าเกนความรู้สูงที่สุด ที่ซึ่งจะเป็นการเลือกแอทริบิวที่ต้องการข้อมูลที่น้อยที่สุดในการระบุ หรือแบ่งข้อมูลออกเป็นชุดข้อมูลย่อย หากไม่เข้าเงื่อนไขในการคำนวณดังกล่าวโปรแกรมจะไม่คัดเลือกปัจจัยเข้าไปเป็นส่วนหนึ่งของต้นไม้ตัดสินใจ หรือสามารถกล่าวสรุปได้ว่า แบบจำลองที่ผู้วิจัยพัฒนาขึ้น ผู้ตอบแบบสอบถามส่วนใหญ่ตอบคำถามในข้อรายได้ไปในทิศทางเดียวกันมากเกินไป หรือกระจายมากเกินไป ทำให้ไม่สามารถนำมาสร้างเป็นปัจจัยในต้นไม้ตัดสินใจได้

5.2.1.2 สำหรับผลการศึกษาในด้านปัจจัยการสื่อสาร ผู้วิจัยนำทฤษฎีหลักของการสื่อสาร มาเป็นกรอบแนวคิดในการวิจัย เพื่อวิเคราะห์ตามกระบวนการสื่อสาร ซึ่งประกอบไปด้วย 4 องค์ประกอบได้แก่ ผู้ส่งสาร (Sender) สาร (Messages) ช่องทาง (Channel) และ ผู้รับสาร (Receiver) โดยมุ่งอธิบายถึงกระบวนการหรือความสามารถของผู้ส่งสาร ว่าจะมีต้องมีทักษะการ

สื่อสาร ทัศนคติ ระดับความรู้ และระดับสังคมวัฒนธรรม ที่ใกล้เคียงกับผู้รับสาร เพื่อให้ผู้รับสารสามารถเข้าใจและตีความสารเหล่านั้นได้

แต่การศึกษาในงานนี้ ผู้วิจัยได้เลือกตัดปัจจัยทางด้านช่องทาง (Channel) ออก เนื่องจากสถานการณ์การแพร่ระบาดของโรคโควิด-19 ประกอบกับภาครัฐ ภาคเอกชน และภาคการศึกษามีการปรับนโยบายการทำงานเป็นรูปแบบวิถีใหม่ ซึ่งมีการศึกษาในต่างประเทศพบว่า การล่อลวงบนอินเทอร์เน็ตมีแนวโน้มสูงขึ้นกว่าช่วงสถานการณ์ปกติ เนื่องจากทุกคนจำเป็นจะต้องใช้สื่ออินเทอร์เน็ตเพื่อการเรียนและการทำงาน ดังนั้นผู้วิจัยจึงสนใจเฉพาะช่องทางสื่อดิจิทัลเท่านั้น

ทั้งนี้ ผลการศึกษาพบว่า 3 องค์ประกอบทั้งผู้ส่งสาร (Sender) สาร (Messages) และผู้รับสาร (Receiver) มีผลต่อการถูกล่อลวงทั้งสิ้น โดยสามารถสังเคราะห์ปัจจัยออกมาได้ทั้งหมด 9 ปัจจัย ดังนี้

ด้านผู้ส่งสาร (Sender) ค้นพบปัจจัยที่เกี่ยวข้องทั้งหมด 2 ปัจจัย ประกอบด้วย การอ้างเป็นบุคคลสำคัญ (Claiming to be an important person) และการสร้างความน่าเชื่อถือ (Credibility) ทั้งนี้อาจเป็นเพราะทั้ง 2 ปัจจัยข้างต้น ล้วนเป็นปัจจัยที่สนับสนุนและส่งเสริมผู้ส่งสารทั้งสิ้น เช่น การที่มิจฉาชีพอ้างเป็นเจ้าหน้าที่ของภาครัฐ มีบัตรประจำตัว มีรูปโปรไฟล์ใส่ชุดข้าราชการ ทำให้เกิดความน่าเชื่อถือตามมา ซึ่ง Sasser (2014) อธิบายว่า หากผู้ส่งและผู้รับเกิดการยอมรับซึ่งกันและกันแล้ว ผู้ฟังก็มักจะคล้อยตามได้โดยง่าย ในทางตรงกันข้าม หากผู้รับไม่เกิดทัศนคติที่ดี เกิดความเชื่อถือต่อผู้พูดแล้ว ก็จะมีความคิดเห็นที่ขัดแย้งกัน ซึ่งการที่มิจฉาชีพสามารถทำให้ผู้รับสารสามารถคล้อยตามได้แล้ว จะเป็นสะพานข้ามไปสู่ความกลัว หรือความโลภต่อไป ซึ่งสอดคล้องกับการศึกษาของ ฐิติมา อินกล่ำ (2558) ที่ได้ศึกษาวาทกรรมทางการสื่อสารเพื่อการหลอกลวงการทำธุรกรรมทางการเงินออนไลน์ผ่านเครื่องอิเล็กทรอนิกส์ พบว่า ปัจจัยด้านการอ้างเป็นบุคคลสำคัญ และ ปัจจัยด้านการสร้างความน่าเชื่อถือ มีผลต่อการถูกล่อลวงทั้งสิ้น โดยพบว่ามิจฉาชีพ (ผู้ส่งสาร) นิยมอ้างเป็น เจ้าหน้าที่ธนาคาร เจ้าหน้าที่ตำรวจ เจ้าหน้าที่ DSI เจ้าหน้าที่ธนาคารแห่งประเทศไทย และเจ้าหน้าที่กรมสรรพกร โดยจะทำการสร้างความน่าเชื่อถือให้กับตนเอง ตั้งแต่การสร้างโปรไฟล์บนโซเชียล การใช้ระบบตอบรับอัตโนมัติ เป็นต้น ทั้งนี้ยังพบอีกว่ามิจฉาชีพมักฉวยโอกาสใช้สถานการณ์บ้านเมืองมาเป็นประเด็นตั้งต้นในการเริ่มการหลอกลวง เช่น การแอบอ้างเป็นหน่วยงานด้านสาธารณสุขที่พร้อมให้ความช่วยเหลือประชาชนจากสถานการณ์การแพร่ระบาดของโควิด-19 อีกด้วย (ไทยรัฐออนไลน์, 2563)

ด้านสาร (Messages) ค้นพบปัจจัยที่เกี่ยวข้องทั้งหมด 3 ปัจจัย ประกอบด้วย กระตุ้นความสนใจ (Arouse interest) กระตุ้นความต้องการ (Stimulate demand) และสร้างความคาดหวัง (Create expectations) ทั้งนี้อาจเป็นเพราะทั้ง 3 ปัจจัยข้างต้นเกี่ยวข้องกับประเภทเนื้อหาที่มิจฉาชีพจะใช้เป็นแรงจูงใจแก่ผู้รับ ซึ่ง Sasser (2014) อธิบายว่า องค์ประกอบของสารจะประกอบไปด้วย 3 ส่วนคือ เนื้อหา สัญลักษณ์ รวมถึงวิธีการส่งข่าวสาร โดยหากมิจฉาชีพมีทักษะในการสื่อสารที่ดี เรียบเรียงถ้อยคำสำนวนที่ถูกต้อง น่าอ่าน และฝั่งผู้รับสารก็มีทักษะในการฟังที่ดี เข้าใจสิ่งที่ผู้ส่งต้องการสื่อ และถอดรหัสสารนั้นได้ ก็จะทำให้การสื่อสารนั้นประสบความสำเร็จ ซึ่งในกรณีนี้คือการที่มิจฉาชีพสามารถสร้างสาร โดยใช้เนื้อหาที่กระตุ้นทั้งความสนใจ ความต้องการ และความคาดหวังมาเป็นตัวการที่ทำให้ผู้รับสารตกเป็นเหยื่อในการถูกล่อลวง ดังเช่น กรณีของเหยื่อที่ได้รับ SMS แจ้งให้อัปเดตข้อมูลกับธนาคารทันทีเพื่อป้องกันบัญชีสูญหาย ซึ่งมิจฉาชีพได้นำข้อมูลที่เหยื่อกรอกเข้ามาในเว็บไซต์ปลอมที่ตนสร้างขึ้นไปถอนเงินผ่านตู้เอทีเอ็ม หรือแอปพลิเคชัน คิดเป็นมูลค่าความเสียหายรวมกว่า 1.9 ล้านบาท (พีพีทีวีออนไลน์, 2563)

ซึ่งพงศ์พนธ์ ภาวศุทธิ์ (2561) ศึกษาสาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคมของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล อธิบายว่ากระบวนสร้างสารที่ใช้ภาพ และเนื้อหาที่กระตุ้นความรู้สึกของผู้รับสาร เป็นอีกสาเหตุสำคัญที่ทำให้การล่อลวงสำเร็จผล โดยเทคนิคส่วนใหญ่ที่มิจฉาชีพนิยมใช้ในการสร้างสารรูปแบบนี้คือการใช้ถ้อยคำที่จำกัดระยะเวลา เช่น ด่วน ทันที รีบดูก่อนโดนลบ ถูกดำเนินคดีทันที อัปเดตก่อนบัญชีจะถูกอายัด กดยกเลิกสินค้าหากคุณไม่ได้สั่งภายใน 15 นาที เป็นต้น

ทั้งนี้ยังพบมิจฉาชีพใช้วิธีการสร้างความคาดหวัง วาดฝันเพื่อให้เหยื่อหลงเชื่อและปฏิบัติตาม เช่น การบอกเหยื่อว่าเป็นผู้โชคดีได้รับรางวัลพิเศษ อาทิ โทรศัพท์มือถือ แท็บเล็ต หรือทองคำ แต่มีเงื่อนไขคือต้องกรอกแบบสอบถาม ต้องส่ง SMS หรือโอนเงินเป็นค่ามัดจำให้กับมิจฉาชีพก่อน ซึ่งสอดคล้องกับการศึกษาของ Aburrous (2010) ที่ได้ศึกษาการพยากรณ์เว็บไซต์ฟิชชิ่งด้วยเทคนิคเหมืองข้อมูล พบว่าโมเดลที่พัฒนาขึ้นมีข้อมูลบนเว็บไซต์อย่างน้อย 6 ประเภท ประกอบด้วย โดเมนของเว็บไซต์ การตั้งค่าความปลอดภัยของเว็บไซต์ โค้ดที่ใช้เขียนเว็บไซต์ ช่องกรอกเว็บไซต์ ปัจจัยส่วนบุคคล และเนื้อหา โดยเฉพาะอย่างยิ่งหากเนื้อหาสร้างความคาดหวังให้แก่อ่าน จะทำให้มิจฉาชีพมีโอกาสสูงขึ้นในการที่จะล่อลวงข้อมูลหรือเงินมัดจำจากเหยื่อ

ด้านผู้รับสาร (Receiver) ค้นพบปัจจัยที่เกี่ยวข้องทั้งหมด 4 ปัจจัย ประกอบด้วย ความกลัว (Fear) ความโลภ (Greed) ความอยากรู้อยากเห็น (Curiosity) และ การตัดสินใจอย่างไม่มี

เหตุผล (Unreasonably Decision) ทั้งนี้อาจเป็นเพราะทั้ง 4 ปัจจัยส่งผลด้านลบต่อผู้รับสาร ทำให้ผู้รับเกิดพฤติกรรมอันตรายเกิดขึ้น ซึ่งสุทธิรักส์ ศุขเขษม (2563) ที่ได้ศึกษาเรื่องปัจจัยทางบุคลิกภาพที่มีผลต่อความเสี่ยงในการโจมตีด้วยระบบสารสนเทศด้วยวิธีวิศวกรรมสังคม พบว่าทั้งความอยากรู้อยากเห็น ความกลัว และความโลภ มีผลต่อการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม

ซึ่งสอดคล้องกับ พงศ์พนธ์ ภาวศุทธิ์ (2563) ที่พบว่านอกจาก 3 ปัจจัยข้างต้น ยังมีอีกหนึ่งปัจจัยนั่นก็คือการตัดสินใจอย่างไม่มีเหตุผล มีผลต่อการถูกโจมตีเช่นเดียวกัน ซึ่งความเชื่อมโยงกับงานวิจัยฉบับนี้ที่มุ่งศึกษาการถูกล่อลวงบนสื่อดิจิทัล เนื่องจากการโจมตีด้วยวิธีการวิศวกรรมสังคม หรือ Social Engineering เป็นภาพใหญ่ที่ใช้เรียกวิธีการล่อลวงเหยื่อบนสื่อดิจิทัล โดยมิจฉาชีพจะอาศัยหลักจิตวิทยา ความไม่รู้หรือความประมาทของเหยื่อ เพื่อหลอกขอข้อมูล อาทิ รหัสผ่าน รหัสบัตรประชาชน รหัสบัตรเครดิต

Social Engineer, LLC. (2021) อธิบายว่ามีการโจมตีด้วยวิธีวิศวกรรมสังคมอยู่หลายเทคนิคที่มิจฉาชีพที่นิยมใช้ อาทิ Phishing การแอบอ้างเป็นองค์กรหรือเว็บไซต์ เพื่อล้วงข้อมูลจากเหยื่อ ซึ่งเป็นวิธีหลักที่ผู้วิจัยต้องการศึกษาในงานวิจัยชิ้นนี้ นอกจากนี้ยังมีเทคนิค อาทิ Baiting การล่อให้เหยื่อเกิดพฤติกรรมอันตราย Scareware การแจ้งเตือนภัยอันตรายปลอมเพื่อกระตุ้นให้เหยื่อติดตั้งซอฟต์แวร์อันตรายลงบนเครื่อง Pretexting การสร้างความไว้เนื้อเชื่อใจให้เหยื่อเปิดเผยข้อมูลสำคัญ และการทำ Mining Social Media การเรียนรู้และเก็บข้อมูลพฤติกรรมส่วนตัวของเหยื่อจากกิจกรรมบนโลกออนไลน์ เพื่อนำมาทำชุดข้อมูลหลอกให้เหยื่อหลงเชื่ออีกครั้งหนึ่ง เป็นต้น

จากข้อมูลดังกล่าวจะพบว่า ปัจจัยที่เกี่ยวข้องกับการสื่อสารทั้ง 9 ปัจจัย ได้แก่ อ้างเป็นบุคคลสำคัญ การสร้างความน่าเชื่อถือ กระตุ้นความสนใจ กระตุ้นความต้องการ สร้างความคาดหวัง ความกลัว ความโลภ ความอยากรู้อยากเห็น และการตัดสินใจอย่างไม่มีเหตุผล มีผลต่อการถูกล่อลวงบนสื่อดิจิทัลทั้งสิ้น สอดคล้องกับข้อมูลจาก Social Engineer, LLC. (2021) ที่รวบรวมข้อมูลด้านการโจมตี ปัจจัยที่ส่งผลให้การโจมตีสำเร็จผล รวมไปถึงกรอบแนวคิดต่าง ๆ พบว่าปัจจัยด้านการสื่อสารเป็นหนึ่งในปัจจัยที่ทำให้มิจฉาชีพสามารถล่อลวงและหลอกขอข้อมูลจากผู้รับสารได้ เพราะในการล่อลวงที่ประสบความสำเร็จ ข้อความที่ถูกส่งออกไปจะสอดคล้องหรือใกล้เคียงกับความตั้งใจของผู้รับสาร อย่างไรก็ตาม มิจฉาชีพหรือส่งจะทราบเพียงข้อความที่สามารถหลอกล่อได้เท่านั้น ไม่สามารถคาดเดาหรือรับรู้ข้อความที่หลอกล่อไม่สำเร็จได้ ซึ่งสอดคล้องกับ Mouton (2014) ที่ได้ศึกษา โมเดลการจำแนกการโจมตีด้วยวิธีวิศวกรรมสังคม พบว่า ปัจจัยด้านการสื่อสาร

ส่งผลให้การโจมตีด้วยวิธีวิศวกรรมสังคมประเภทการโจมตีโดยตรงสำเร็จผล แต่ไม่มีผลกับการโจมตีทางอ้อม สิ่งที่มีผลกับการโจมตีทางอ้อมคือช่องทางเท่านั้น

ทั้งนี้จากการศึกษาเพิ่มเติมยังพบว่า นอกเหนือจาก 9 ปัจจัยข้างต้นที่ส่งผลต่อความเสี่ยงในถูกล่อลวง ผลการศึกษาของ พงศ์พนธ์ ภาวศุทธิ์ (2563) ยังชี้ให้เห็นอีกว่ามีบางปัจจัยที่ช่วยลดความเสี่ยงต่อการถูกล่อลวง อาทิ การรับรู้ภัยคุกคาม ประสบการณ์ก่อนหน้า และการแจ้งเตือนจากผู้ที่รู้จัก หากผู้ใช้งานสื่อดิจิทัลมีความตระหนัก และมีการเพิ่มพูนทักษะในการเฝ้าระวัง ตรวจสอบสิ่งผิดปกติ ก็จะช่วยลดโอกาสในการถูกโจมตีได้มากยิ่งขึ้น ในด้านช่องทาง (Channel) ที่ผู้วิจัยไม่ได้ทำการศึกษาในครั้งนี้ ยังมีการพบการถูกล่อลวงด้วยวิธีคล้ายคลึงกับการถูกล่อลวงบนสื่อดิจิทัล เช่นเดียวกัน อาทิ แก๊งค์คอลเซ็นเตอร์ ที่ใช้การล่อลวงผ่านเสียง สอบถามข้อมูลของเหยื่อ และให้เหยื่อปฏิบัติตามคำแนะนำอันตรายของตน หรือการล่อลวงผ่าน SMS สั้น โดยให้คลิกลิงก์ หรือติดตั้งแอปอันตรายลงบนเครื่อง

5.2.2 จากวัตถุประสงค์ “เพื่อพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล”

ผลการพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล จะมีค่าความถูกต้อง (Accuracy) มากที่สุด เมื่อสร้างโดยใช้เทคนิคต้นไม้ตัดสินใจ ด้วยวิธีการแบ่งชุดข้อมูลการเรียนรู้และทดสอบออกจากกัน 80:20 โดยได้ผลลัพธ์หรือเงื่อนไขในรูปแบบกฎทั้งสิ้น 118 กฎ โดยสามารถนำแบบจำลองและกฎดังกล่าวไปใช้สำหรับการคาดการณ์ พยากรณ์ หรืออธิบายถึงสาเหตุของปัญหาการถูกล่อลวงบนสื่อดิจิทัลของกลุ่มคนดิจิทัลเนทีฟ ที่มีอายุระหว่าง 18-36 ปี ว่าเกิดจากพฤติกรรม หรือปัจจัยใดที่ทำให้ถูกล่อลวง รวมถึงยังสามารถนำไปปรับใช้เป็นบทเรียน เพื่อแก้ไขปัญหาการถูกล่อลวงบนสื่อดิจิทัลในอนาคตได้อย่างตรงจุดมากยิ่งขึ้น

นอกจากนี้ การพัฒนาแบบจำลองดังกล่าว ผู้วิจัยเน้นเปรียบเทียบเฉพาะค่าความถูกต้อง (Accuracy) ถูกต้องเท่านั้น ซึ่งวิธีการคัดเลือกวิธีการสร้างแบบจำลองที่ดีที่สุด สอดคล้องกับ รัชพล กลัดชื่น (2018) ที่ได้ศึกษาการเปรียบเทียบประสิทธิภาพอัลกอริทึมและการคัดเลือกคุณลักษณะที่เหมาะสมเพื่อการทำนายผลสัมฤทธิ์ทางการเรียนของนักศึกษาระดับอาชีวศึกษา โดยใช้เทคนิคการจำแนก 3 เทคนิค ได้แก่ ต้นไม้ตัดสินใจ J48 นาอีฟเบย์ และเทคนิคกฎการอุปนัย การคัดเลือกดังกล่าวใช้ค่าความถูกต้อง (Accuracy) ในการนำเสนอแบบจำลอง ซึ่ง Li (2018) ที่ได้ศึกษา

การเปรียบเทียบแบบจำลองการทำเหมืองข้อมูลสามแบบสำหรับการพยากรณ์โรค Schistosomiasis ขั้นสูงในมลฑลหูเป่ย ก็ได้ใช้การเปรียบเทียบโดยใช้ค่าความถูกต้อง (Accuracy) เช่นเดียวกัน

5.3 ข้อเสนอแนะเพื่อการวิจัย

5.3.1 ข้อเสนอแนะในการนำไปใช้

5.3.2.1 ผลจากการวิจัยครั้งนี้ทำให้ได้แบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล ซึ่งนำไปใช้วัดเพื่อเป็นข้อมูลในการจัดกิจกรรม ส่งเสริมความรู้ และการใช้งานอินเทอร์เน็ตให้กับหน่วยงานที่เกี่ยวข้องในการดูแลสังคมให้ปลอดภัย

5.3.2.2 ในการนำแบบจำลองไปใช้งาน ควรมีการกำหนดขอบเขตของอายุ และผู้รับสารให้สอดคล้องกับงานวิจัย เพื่อให้ประชาชนเกิดความรู้เท่าทันภัยฟิชชิ่ง มีองค์ความรู้ในการเลือกและตัดสินใจการเข้าถึงข้อมูลสื่อดิจิทัลประเภทต่าง ๆ

5.3.2 ข้อเสนอแนะในการวิจัย

5.3.2.1 ควรมีการศึกษาในกลุ่มเป้าหมายที่เฉพาะเจาะจง อาทิ กลุ่มผู้สูงอายุ และกลุ่มเด็กวัยประถมศึกษา เพื่อนำมาหาความเชื่อมั่นของแบบวัดให้ครอบคลุมกลุ่มเป้าหมายที่เกี่ยวข้องได้เพิ่มขึ้น

5.3.2.2 การศึกษาครั้งต่อไปควรทำการศึกษาวิจัยเชิงคุณภาพ เพื่อให้ได้ข้อมูลเชิงลึกในเรื่องการตัดสินใจและความคิดเห็นของกลุ่มเป้าหมาย ในการสร้างแบบจำลองบูรณาการร่วมกับการทบทวนวรรณกรรมเพิ่มเติม

บรรณานุกรม

บรรณานุกรม

ภาษาไทย

กษิดิศ สตางค์มงคล. (2562). *รีวิวสูตรคำนวณจำนวนตัวอย่างของ อ.*Taro Yamane. สืบค้น 2 พฤษภาคม 2564, จาก https://datarockie.com/2019/08/23/yamane-sample-size-calculation/

กันต์นลิน เปรมใจสุข. (2562). *อิทธิพลของปัจจัยการสื่อสารแบบบอกต่อที่มีผลต่อพฤติกรรมผู้บริโภคในธุรกิจอิเล็กทรอนิกส์.* [วิทยานิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. http://cuir.car.chula.ac.th

โกเมศ อัมพวัน. (2553). *บทที่ 6 การจำแนกประเภทและการทำนายข้อมูล. สืบค้น 2 พฤษภาคม 2564*, จาก https://staff.informatics.buu.ac.th/~komate/886464/%5B6%5D-Classification.pdf

กุลธิดา อาธิเจริญสุข. (2559). *การบังคับใช้กฎหมายเกี่ยวกับฟิชชิ่ง.* [วิทยานิพนธ์ปริญญามหาบัณฑิต, สถาบันบัณฑิตพัฒนบริหารศาสตร์]. http://library.nida.ac.th

จินตนา โนนวงศ์. (2558). *ปัจจัยที่ส่งผลต่อการตัดสินใจเลือกแผนการเรียนของนักเรียนชั้นมัธยมศึกษาปีที่ 3 : การวิเคราะห์จำแนกกลุ่มและการวิเคราะห์ซัพพอร์ตเวกเตอร์แมชชีน.* [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยมหาสารคาม]. https://library.msu.ac.th/

จินตนา เหมรา. (2558). *การสื่อสารเกี่ยวกับการป้องกัน HIV สำหรับผู้ต้องขังในเรือนจำ.* [วิทยานิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. http://cuir.car.chula.ac.th

จิรา แก้วสุวรรณ์. (2549). *การตรวจจับและแก้ไขการวางตัวของภาพโดยใช้ซัพพอร์ตเวกเตอร์แมชชีน.* [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ]. http://www.gits.kmutnb.ac.th/thesis

ชัยชนะ กุลวรฐิต. (2563). *การพัฒนาระบบสังเคราะห์ความสัมพันธ์ของปัจจัยที่ส่งผลต่อความฉลาดทางดิจิทัลด้วยเทคนิคเหมืองข้อมูล.* [วิทยานิพนธ์ปริญญาดุษฎีบัณฑิต, สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารหลาดกระบัง]. http://thesis.lib.kmitl.ac.th

ชานนท์ สำเภาอินทร์. (2557). *ความรับผิดในการขู่เข็ญให้ผู้อื่นเกิดความกลัว.* [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์]. https://library.tu.ac.th/th/e-thesis

ฐิติมา อินกล่ำ. (2558). *วาทกรรมทางการสื่อสารเพื่อการหลอกลวงทำธุรกรรมทางการเงินออนไลน์ผ่านเครื่องอิเล็กทรอนิกส์*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยแม่โจ้]. https://library.mju.ac.th/mjudc

ณิศรา ศรีพลอยรุ่ง. (2558). *การใช้สื่อดิจิทัลด้านการท่องเที่ยวของกลุ่มดิจิทัลเนทีฟไทย*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. http://cuir.car.chula.ac.th

ดารารัตน์ ภูธร. (2561). การตระหนักรู้ของดิจิทัลเนทีฟไทยต่อการละเมิดลิขสิทธิ์การ์ตูนและแอนิเมชันญี่ปุ่นออนไลน์. *วารสารการสื่อสารและการจัดการ นิด้า, 4*(2).

ตฤณ ทวิธารานนท์. (2562). *บทบาทของโซเชียลมีเดียในการลงโทษทางสังคม*. [วิทยานิพนธ์ปริญญาดุษฎีบัณฑิต, มหาวิทยาลัยรังสิต]. http://library.rsu.ac.th/library_thesis.html

ไทยเซิร์ต. (2563). *แจ้งเตือนพบการส่ง SMS หลอกให้ดาวน์โหลดแอปพลิเคชัน ไทยชนะ แท้จริงเป็นมัลแวร์ขโมยข้อมูลทางการเงิน*. สืบค้น 10 พฤศจิกายน 2563, จาก https://www.thaicert.or.th/newsbite/2020-05-23-01.html

ไทยรัฐออนไลน์. (2563ก). *“จ๊ะจ๋า พริมรตา” ควง “จิ๊บ วสุ” โร่ร้อง ปอท. โดนแฮกเกอร์ยึดไอจี*. สืบค้น 2 พฤษภาคม 2564, จาก https://www.thairath.co.th/news/crime/1866499

ไทยรัฐออนไลน์. (2563ข). *เตือนทั่วโลกระวังอีเมลหลอกเช็กเงินเยียวยา*. สืบค้น 2 พฤษภาคม 2564, จาก https://www.thairath.co.th/news/tech/1845934

ไทยรัฐออนไลน์. (2563ค). *รวบตัว ส.ส.สอบตก แจกมือถือตุ๋นนักธุรกิจ*. สืบค้น 2 พฤษภาคม 2564, จาก https://www.thairath.co.th/news/local/bangkok/1861521

ไทยรัฐออนไลน์. (2564ง). *ยายฮ่องกงร้องโดนแก๊งต้มตุ๋นปลอมเป็น จนท. หลอกโอนเงิน 1,000 ล้านบาท*. สืบค้น 2 พฤษภาคม 2564, จาก https://www.thairath.co.th/news/foreign/2074323

ไทยรัฐออนไลน์. (2564จ). *สตม.รวบแก๊งลวงเป็น จนท.แบงก์ หลอกนำข้อมูล ตุ๋นเงิน 20 ราย กว่า 2 ล้าน*. สืบค้น 2 พฤษภาคม 2564, จาก https://www.thairath.co.th/news/crime/2012643

ธงชัย แก้วกิริยา. (2558). *การสังเคราะห์รูปแบบแนะนำผู้เรียนอีเลิร์นนิ่งแบบปรับเหมาะตามการวิเคราะห์พหุปัญญาและข้อมูลผู้เรียนที่วิเคราะห์ด้วยเหมืองข้อมูล*. [วิทยานิพนธ์ปริญญาดุษฎีบัณฑิต, มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ]. http://www.gits.kmutnb.ac.th/thesis

ธนกร เจริญเชาว์. (2554). *ระบบสนับสนุนการเสนอขายคอนโดมิเนียม โดยใช้เทคนิคนาอีฟเบย์เซียน*. [วิทยานิพนธ์ปริญญามหาบัณฑิต,มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ]. http://www.gits.kmutnb.ac.th/thesis

ธนัท สมณคุปต์. (2562). การสื่อสารผ่านสื่อดิจิทัลของวิสาหกิจชุมชน. วารสารเทคโนโลยีและสื่อสารการศึกษา. *ECT Journal, 16*.

ธรรมสรณ์ นูมหันต์. (2558). *การวิเคราะห์ข้อมูลและการพยากรณ์เพื่อสนับสนุนการตัดสินใจในธุรกิจยานยนต์*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ]. http://www.gits.kmutnb.ac.th/thesis

นิพัทธา อินทรักษา. (2560). *การเล่าเรื่องประเด็นสังคมผ่านคลิปวิดีโอบนสื่อออนไลน์*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. http://cuir.car.chula.ac.th

เบญจพร ลิ้มธรรมาภรณ์. (2554). การตรวจจับบอทเน็ตสแปมเมล์และความตระหนักในภัยลวงเฟซบุ๊กฟิชชิ่ง. *วารสารวิชาการพระจอมเกล้าพระนครเหนือ*, *21(3)*.

ปรมะ สตะเวทิน. (2546). *หลักนิเทศศาสตร์*. (พิมพ์ครั้งที่ 10). กรุงเทพฯ: ภาควิชาการประชาสัมพันธ์ คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

ประภัสสร ศรีสด. (2558). *ปัจจัยที่มีอิทธิพลต่อการตัดสินใจซื้อผลิตภัณฑ์การท่องเที่ยวผ่านเว็บไซต์ร่วมกันซื้อ*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. http://cuir.car.chula.ac.th

ปวันตา บุญพันธ์. (2557). *การศึกษาความรู้สึกหวาดกลัวอาชญากรรมของผู้สูงอายุในเขตลาดพร้าว กรุงเทพมหานคร*. [สารนิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์]. https://library.tu.ac.th/th/e-thesis

ปวีณา ชัยวนารมย์ (2558). *การพัฒนาแบบจำลองเพื่อพยากรณ์โอกาสการเกิดความเครียดในหลายระดับด้วยเทคนิคการทำเหมืองข้อมูล*. [มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์]. https://www.rmutr.ac.th/research/

ปาริชาต สถาปิตานนท์. (2551). *การสื่อสารประเด็นสาธารณะและการเปลี่ยนแปลงในสังคมไทย*. กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

พงศ์พนธ์ ภาวศุทธิ์. (2561). *สาเหตุเชิงลึกของการถูกโจมตีด้วยวิธีการทางวิศวกรรมสังคม ของกลุ่มเจเนอเรชั่นวาย ในเขตกรุงเทพมหานครและปริมณฑล*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์]. https://library.tu.ac.th/th/e-thesis

พรพล ธรรมรงค์รัตน์. (2552). *การจำแนกประเภทเว็บเพจโดยวิธีการลดขนาดลักษณะเฉพาะและซัพพอร์ตเวกเตอร์แมชชีน*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยสงขลานครินทร์]. https://gradmis.psu.ac.th/Thesis

พรรณี ลีกิจวัฒนะ. (2559). *การวิจัยทางการศึกษา*. (พิมพ์ครั้งที่ 11). กรุงเทพฯ: มีน เซอร์วิส ซัพพลาย.

พีพีทีวีออนไลน์. (2563ก). *ผู้เสียหายสงสัย ข้อมูลหลุดจากธนาคาร ต้นเหตุถูกแฮ็กเงินในบัญชี*. สืบค้น 2 พฤษภาคม 2564, จาก https://www.pptvhd36.com/news/อาชญากรรม/138206

พีพีทีวีออนไลน์. (2563ข). *มิจฉาชีพ อ้างเป็นทนายหลอกให้โอนเงิน 4 แสน*. สืบค้น 2 พฤษภาคม 2564, จาก https://www.pptvhd36.com/news/ประเด็นร้อน/130638

พีรญา ดุนขุนทด. (2553). *ระบบช่วยแนะนำสำหรับการดูแลช่วยเหลือนักเรียน โดยการจำแนกข้อมูลด้วยเทคนิค Suuport Vector Machine กรณีศึกษาโรงเรียนมัธยมวัดมกุฎกษัตริย์*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ]. http://www.gits.kmutnb.ac.th/thesis

ภัทราพร ช่างจูม. (2554). *การจำแนกพืชสมุนไพรตามลักษณะภายนอกด้วยวิธีการนาอีฟเบย์*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ]. http://www.gits.kmutnb.ac.th/thesis

วรวุฒิ อ่อนน่วม. (2559). ปรากฏการณ์ทางการสื่อสารยุคดิจิทัล. *วารสารวิชาการสมาคมสถาบันอุดมศึกษาเอกชนแห่งประเทศไทย (สสอท.)*.

รัชพล กลัดชื่น. (2018). การเปรียบเทียบประสิทธิภาพอัลกอริทึมและการคัดเลือกคุณลักษณะที่เหมาะสมเพื่อการทำนายผลสัมฤทธิ์ทางการเรียนของนักศึกษาระดับอาชีวศึกษา. *วารสารวิจัย มหาวิทยาลัยเทคโนโลยีราชมงคลธัญบุรี*, *17*(1).

ศุภกร จูฑะพล. (2557). *ทัศนคติ พฤติกรรม และความคล่องดิจิทัลของกลุ่มดิจิทัลเนทีฟ*. (ศิลปศาสตร์มหาบัณฑิต). [วิทยานิพนธ์ปริญญามหาบัณฑิต, สถาบันบัณฑิตพัฒนบริหารศาสตร์]. http://library.nida.ac.th

ศุภชัย ประคองศิลป์. (2551). *การออกแบบและพัฒนาระบบสนับสนุนการตัดสินใจในการอนุมัติลูกบ้านเข้าโครงการโดยใช้เทคนิคต้นไม้ตัดสินใจ กรณีศึกษา มูลนิธิที่อยู่อาศัยเพื่อมนุษยชาติ*. [ปัญหาพิเศษปริญญามหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ]. http://www.gits.kmutnb.ac.th/thesis

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต). (2563). *สถิติภัยคุกคาม 2563*. สืบค้น 8 ตุลาคม 2563, จาก https://www.thaicert.or.th/statistics/statistics.html

สสินาท แสงทองฉาย. (2560). *ปัจจัยส่วนประสมทางการตลาดที่มีอิทธิพลต่อพฤติกรรมของผู้บริโภคกลุ่มดิจิทัลเนทีฟไทยในการเลือกใช้แอปพลิเคชันสั่งและจัดส่งอาหารในเขต*

กรุงเทพมหานคร. [วิทยานิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. http://cuir.car.chula.ac.th

สำนักงานสถิติแห่งชาติ. (2562). *สำรวจการมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารในครัวเรือน พ.ศ. 2562.* สืบค้น 10 พฤศจิกายน 2563, จาก http://www.nso.go.th/sites/2014/DocLib13/ด้านICT/เทคโนโลยีในครัวเรือน/2562/Pocketbook_2562.pdf

สุดารัตน์ วงศ์คำ. (2557). *การศึกษาวิเคราะห์คำสอนเรื่องโลภะในพระพุทธศาสนาเถรวาท*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยธรรมศาสตร์]. https://library.tu.ac.th/th/e-thesis

สุทธิรักส์ ศุขเขษม (2563). *ปัจจัยทางบุคลิกภาพที่มีผลต่อความเสี่ยงในการโจมตีระบบสารสนเทศด้วยวิศวกรรมสังคม.* งานประชุมวิชาการระดับชาติ ครั้งที่ 12 มหาวิทยาลัยราชภัฏนครปฐม.

สุนันทา เรียงแหลม. (2551). *การศึกษาแก้ปัญหาความโลภในสังคมปัจจุบันตามหลักพระพุทธศาสนาเถรวาท*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, มหาวิทยาลัยมหาจุฬาลงกรณ์ราชวิทยาลัย]. http://oldweb.mcu.ac.th/site/thesiscontent.php

สุพัตรา สถิตย์จันทรากุล. (2552). *มาตรการทางอาญาในการป้องกันเด็กและเยาวชนจากการถูกล่อลวงในทางเพศโดยอาศัยอินเทอร์เน็ตหรือการสื่อสารทางอิเล็กทรอนิกส์เป็นเครื่องมือ*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. http://cuir.car.chula.ac.th

สุรชัย ฉัตรเฉลิมพันธุ์. (2563). *ความมั่นคงปลอดภัย: กรณีศึกษาการรู้เท่าทันภัยทางไซเบอร์ของผู้บริหารในสถาบันการเงินโดยการจำลองการโจมตีด้วยฟิชชิ่ง*. The Sixteenth National Conference on Computing and Information Technology.

อริสสา สชิวิลเลอร์. (2559). *กระบวนการสื่อสารเพื่อการรณรงค์บริจาคสเต็มเซลล์ของสภากาชาดไทย*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, จุฬาลงกรณ์มหาวิทยาลัย]. http://cuir.car.chula.ac.th

อัณศยา เกิดคล้าย. (2553). การตรวจจับไวรัสข้อความสื่อประสม โดยใช้เทคนิคการทำเหมืองข้อมูล. *Srinakharinwirot Engineering Journal, 5*(2).

เอมิการ์ ศรีธาตุ. (2559). *พฤติกรรมการใช้และการรับรู้อิทธิพลของสื่อดิจิทัลต่อเจเนอเรชั่นวายและเจเนอเรชั่นแซดในเขตกรุงเทพมหานครและปริมณฑล*. [วิทยานิพนธ์ปริญญามหาบัณฑิต, สถาบันบัณฑิตพัฒนบริหารศาสตร์]. http://library.nida.ac.th

ภาษาอังกฤษ

Abroshan, H., Devos, J., Poels, G., & Laermans, E. (2021). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access*, 9, 44928-44949.

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010, 12-14 April 2010). Predicting Phishing Websites Using Classification Mining Techniques with Experimental Case Studies. *2010 Seventh International Conference on Information Technology: New Generations,*

Accenture. (2019). *The cost of cybercrime*. Retrieved October 10, 2020, from https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

Ahmed, M. T., & Omotunde, H. (2012). Theories and strategies of good decision making. *International journal of scientific & technology research, 1*(10), 51-54.

Ainslie, G. (1975). Specious reward: a behavioral theory of impulsiveness and impulse control. *Psychological bulletin, 82*(4), 463.

Albladi, S. M., & Weir, G. R. S. (2017, 23-24 Nov. 2017). *Personality traits and cyber-attack victimisation: Multiple mediation analysis.* Paper presented at the 2017 Internet of Things Business Models, Users, and Networks.

Alseadoon, I., Othman, M., & Chan, T. (2015). What is the influence of users' characteristics on their ability to detect phishing emails? In *Advanced computer and communication engineering technology* (pp. 949-962): Springer.

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185-197.

Berlo, D. K. (1960). *The process of communication; an introduction to theory and practice*. New York: Holt, Rinehart and Winston.

Birkett, A. (2017). *Fear and Greed: What Drives Human Behavior?***.** Retrieved November 28, 2020, from https://cxl.com/blog/fear-and-greed/

Bobby Allyn. (2020). *Twitter Says It Was The Victim Of A 'Coordinated Social Engineering Attack'.* Retrieved October 5, 2020, from https://www.wbez.org/stories/twitter-says-it-was-the-victim-of-a-coordinated-social-engineering-attack

Breda & Berlamont. (2014). *The secret of fear and greed behind financial decision making.* GHENT UNIVERSITY,

Breda, F., Barbosa, H., & Morais, T. (2017). *SOCIAL ENGINEERING AND CYBER SECURITY*.

Cherry, C. (1957). On human communication; a review, a survey, and a criticism.

Cofense. (2020). *History of Phishing.* Retrieved October 10, 2020, from https://resources.infosecinstitute.com/technical-details-reasons-attack/

Dijkstra, J. (2018). *Relation between Dispositional Greed and Impulsive Buying Tendency: Role of Cognitive Reflection.* Tilburg University

Forcepoint. (2017). *7 Cybersecurity Predictions for 2017.* Retrieved November 25, 2020, from https://www.forcepoint.com/2017predictions

Gkioulos, V., Wangen, G., Katsikas, S., Karagiannidis, G., & Kotzanikolaou, P. (2017). Security Awareness of the Digital Natives. *Inf., 8*, 42.

Golman, R., & Loewenstein, G. (2015). Curiosity, information gaps, and the utility of knowledge. *Information Gaps, and the Utility of Knowledge (April 16, 2015)*, 96-135.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345-358.

Griffin, R. (2018). A Demographic Analysis to Determine User Vulnerability among Several Categories of Phishing Attacks.

Halevi, T., Memon, N., & Nov, O. (2015). Spear-phishing in the wild: A real-world study of personality, phishing self-efficacy and vulnerability to spear-phishing attacks. *Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks (January 2, 2015)*.

Han, J., Pei, J., & Kamber, M. (2011). *Data mining: concepts and techniques*: Elsevier.

Harrison, B., Svetieva, E., & Vishwanath, A. (2016). Individual processing of phishing emails. *Online Information Review*.

Harrison, B., Vishwanath, A., Ng, Y. J., & Rao, R. (2015). *Examining the impact of presence on individual phishing victimization.* Paper presented at the 2015 48th Hawaii International Conference on System Sciences.

Hill, K. M., Fombelle, P. W., & Sirianni, N. J. (2016). Shopping under the influence of curiosity: How retailers use mystery to drive purchase motivation. *Journal of Business Research, 69*(3), 1028-1034.

Hooper, V., & Blunt, C. (2020). Factors influencing the information security behaviour of IT employees. *Behaviour & Information Technology, 39*(8), 862-874.

House, D., & Raja, M. K. (2020). Phishing: message appraisal and the exploration of fear and self-confidence. *Behaviour & Information Technology, 39*(11), 1204-1224.

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). Communication and persuasion.

Hughes, R. C. (2018). *Human Capital Systems, Analytics, and Data Mining*: CRC Press.

Inc., T. (2020). *An update on our security incident.* Retrieved November 25, 2020, from https://blog.twitter.com/en_us/topics/company/2020/an-update-on-our-security-incident.html

Inter Telecommunication Union [ITU]. (2013). *Measuring the information society. Geneva: .* Retrieved November 25, 2020, from https://www.itu.int/en/ITU-D/Statistics/Documents/publications/anapub/Youth_2008.pdf

J. Sharp and P.Wu. (2017). *Student Intentions and Behaviors Related to Email Security: An Application of the Health Belief Model.* Paper presented at the Proceedings of the Conference on Information Systems Applied Research ISSN.

Jansen, J., & Van Schaik, P. (2018). Testing a model of precautionary online behaviour: The case of online banking. *Computers in Human Behavior, 87*, 371-383.

Kahneman. (2011). *Thinking, fast and slow*. Toronto: Doubleday Canada.

Kotu, V., & Deshpande, B. (2014). *Predictive analytics and data mining: concepts and practice with rapidminer*: Morgan Kaufmann.

Kozak, J. (2019). Theoretical Framework. In *Decision Tree and Ensemble Learning Based on Ant Colony Optimization* (pp. 1-25). Cham: Springer International Publishing.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications, 22*, 113-122.

Kudyba, S. (2019). *BIG DATA, MINING, AND ANALYTICS : components of strategic decision making*. CRC Press.

Laran, J., & Tsiros, M. (2013). An investigation of the effectiveness of uncertainty in marketing promotions involving free gifts. *Journal of Marketing, 77*(2), 112-123.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.

Limandri, B. (1998). Psychiatric-mental health nurse practitioner with expertise in violence against women and substance abuse. *Journal of Addictions Nursing, 10*(1), 52-54.

Litman, J., & Spielberger, C. (2003). Measuring Epistemic Curiosity and Its Diversive and Specific Components. *Journal of personality assessment, 80*, 75-86.

Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security, 38*, 28-38.

Mahapatra, R. K., & Bose, I. (2001). Business data mining—a machine learning perspective. *Information & management, 39*(3), 211-225.

Mirzakhanov, V. E. (2020). Value of fuzzy logic for data mining and machine learning: A case study. *Expert Systems with Applications, 162*, 113781.

Mitra, S., Pal, S. K., & Mitra, P. (2002). Data mining in soft computing framework: A survey. *IEEE Transactions on Neural Networks, 13*(1), 3-14.

Mouton, F., Leenen, L., Malan, M. M., & Venter, H. S. (2014). Towards an Ontological Model Defining the Social Engineering Domain. In K. Kimppa, D. Whitehouse, T. Kuusela, & J. Phahlamohlaka, *ICT and Society* Berlin, Heidelberg.

Mussel, P., Reiter, A., Osinsky, R., & Hewig, J. (2015). State- and trait-greed, its impact on risky decision-making and underlying neural mechanisms. *Social neuroscience, 10*, 1-9.

Musuva, P. M., Getao, K. W., & Chepken, C. K. (2019). A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility. *Computers in Human Behavior, 94*, 154-175.

Nemati, H. R. (2009). *Techniques and applications for advanced information privacy and security : emerging organizational, ethical, and human issues* Retrieved November 25, 2020, from http://www.myilibrary.com?id=213050

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology, 5*.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology, 5*(1).

Pandey Mayank, & Ravi Vadlamani. (2013). Text and Data Mining to Detect Phishing Websites and Spam Emails. In B. K. Panigrahi, P. N. Suganthan, S. Das, & S. S. Dash, *Swarm, Evolutionary, and Memetic Computing* Cham.

Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. (2009). A personality based model for determining susceptibility to phishing attacks. *Little Rock: University of Arkansas*, 285-296.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? *Information Management & Computer Security, 20*(1), 18-28.

Pimporn Pimpim. (2019). *Classification using Decision Tree.* Retrieved November 27, 2020, from https://medium.com/@doohpim/04-2-classification-using-decision-tree-fc2a7108fe26

Purkait, S., De, S. K., & Suar, D. (2014). An empirical investigation of the factors that influence Internet user's ability to correctly identify a phishing website. *Information Management & Computer Security*.

Reyns, B. W. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*.

Safrudiannur, S. (2020). *Measuring Teachers' Beliefs Quantitatively: Criticizing the Use of Likert Scale and Offering a New Approach*.

Sakaki, M., Yagi, A., & Murayama, K. (2018). Curiosity in old age: A possible key to achieving adaptive aging. *Neurosci Biobehav Rev, 88*, 106-116.

Sasser, S., Kilgour, M., & Hollebeek, L. D. (2014). Marketing in an interactive world: the evolving nature of communication processes using social media. In *Harnessing the Power of Social Media and Web Analytics* (pp. 29-52). IGI Global.

Seuntjens, T. G., Zeelenberg, M., Breugelmans, S. M., & Van de Ven, N. (2015). Defining greed. *British Journal of Psychology, 106*(3), 505-525.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Shu, X. (2020). *Knowledge Discovery in the Social Sciences: A Data Mining Approach*: Univ of California Press.

Simon Kemp. (2020). *DIGITAL **2020**: JULY GLOBAL STATSHOT.* Retrieved November 1, 2020, from https://datareportal.com/reports/digital-2020-july-global-statshot

Social Engineer, I. (n.d.). *The Social Engineering Framework.* Retrieved November 5, 2020, from https://www.social-engineer.org/framework/influencing-others/

Spielberger, C. (2004). *Encyclopedia of applied psychology*: Academic press.

Thaire Group. (2015). *Cyber Insurance Potential In Thailand*. Retrieved November 1, 2020, from https://thaire.co.th/thaire_backend/upload/ourservices/publice_20151216111050.pdf

The European Computer Security Incident Response Team Network. (2003). *WP4 Clearinghouse Policy.* Retrieved November 5, 2020, from http://www.ecsirt.net/cec/service/documents/wp4-clearinghouse-policy-v12.html

Van Schaik, P., & Jansen, J. (2018). Design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human Computer Studies*.

Velayutham, S. (2017). Data Mining and Data Warehousing. In.

Cybersecurity Ventures. (2018). *2019 Official Annual Cybercrime Report*. Retrieved November 25, 2020, from https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586.

Volkenstein, M. V. (2009). *Entropy and information* (Vol. 57): Springer Science & Business Media.

Wang, J., Herath, T., Chen, R., Vishwanath, A., & Rao, H. R. (2012). Research article phishing susceptibility: An investigation into the processing of a targeted spear phishing email. *IEEE transactions on professional communication, 55*(4), 345-362.

Wang, J., Li, Y., & Rao, H. R. (2017). Coping responses in phishing detection: an investigation of antecedents and consequences. *Information Systems Research, 28*(2), 378-396.

Wang, Z. G., Sun, L. M., & Zhu, H. S. (2020). Defining Social Engineering in Cybersecurity. *IEEE Access, 8*, 85094-85115.

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human-Computer Studies*, 120, 1-13.

Workpoint Today. (2563). *อ้างเป็นคนบริษัทมือถือ หลอกขอรหัส OTP 4 หลักเข้าไปโอนเงินกว่า 4 แสน.* Retrieved November 10, 2020, from https://workpointtoday.com/otp/

Wright, R. T., & Marett, K. (2010). The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived. *Journal of Management Information Systems, 27*(1), 273-303.

Yokekung. (2563). *AIS เตือนประชาชนอย่าหลงเชื่อเว็บไซต์ปลอม หลังพบอ้างชื่อบริษัทแจกแบบสอบถามลุ้นรับสมาร์ทโฟน.* Retrieved November 10, 2020, from https://www.adslthailand.com/post/7082

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace. *Information Technology & People*.

ภาคผนวก

ภาคผนวก ก

ผู้ทรงคุณวุฒิ

ผู้ทรงคุณวุฒิในงานวิจัย เรื่อง การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยง ต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล มีดังนี้

1. ผู้ทรงคุณวุฒิ เพื่อประเมินความสอดคล้องระหว่างข้อคำถามกับนิยามศัพท์เฉพาะ จำนวน 3 คน ได้แก่

(1) ผศ.ดร. บุญสิทธิ์ ยิ้มวาสนา ประธานหลักสูตรปรัชญาดุษฎีบัณฑิต สาขาวิทยาการคอมพิวเตอร์ คณะเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยมหิดล

(2) นายพัชรพล สู่สุข ผู้เชี่ยวชาญด้านความปลอดภัยทางระบบคอมพิวเตอร์ บริษัท เอทีเอ ไอที จำกัด

(3) ส.ต.อรรถชัย ไชยวรรณะ นายสิบปฏิบัติการข่าว ชุดปฏิบัติการพิเศษการข่าวที่ 2 ตอนปฏิบัติการข่าว กองพันระวังป้องกัน สำนักงานปลัดกระทรวงกลาโหม

ภาคผนวก ข

การจำแนกค่าตัวแปร

ตารางที่ ค.1 การจำแนกค่าของตัวแปรที่เกี่ยวข้องกับปัจจัยการสื่อสาร

ลำดับ	ปัจจัย	ค่าของตัวแปร
1	เพศ	1. ชาย 2. หญิง 3. กลุ่มบุคคลที่มีความหลากหลายทางเพศ
2	อายุ	1. 18-21 ปี 2. 22-25 ปี 3. 26-29 ปี 4. 30-33 ปี 5. 34-36 ปี
3	ระดับการศึกษา	1. ต่ำกว่าปริญญาตรี 2. ปริญญาตรี 3. ปริญญาโท 4. ปริญญาเอก
4	อาชีพ	1. นักเรียน/นักศึกษา 2. ข้าราชการ/พนักงานรัฐวิสาหกิจ 3. พนักงานบริษัทเอกชน 4. ประกอบธุรกิจส่วนตัว/เจ้าของกิจการ 5. แม่บ้าน/พ่อบ้าน 6. อื่น ๆ โปรดระบุ……..
5	รายได้เฉลี่ยต่อเดือน	1. 5,000 บาท หรือต่ำกว่า 2. 5,001 - 10,000 บาท 3. 10,001 - 15,000 บาท 4. 15,001 – 20,000 บาท 5. 20,001 - 25,000 บาท 6. 25,001 – 30,000 บาท 7. มากกว่า 30,000 บาท

ตารางที่ ค.2 การจำแนกค่าองค์ประกอบที่เกี่ยวข้องกับปัจจัยการสื่อสาร

รายการคำถาม	ค่าองค์ประกอบ
ผู้ส่งสาร (Sender)	
1. อ้างเป็นบุคคลสำคัญ	
1.1 ท่านเชื่อถือข้อมูลเหล่านั้นทันที หากส่งมาจากบุคคลที่รู้จัก	1. เห็นด้วยที่สุด 2. เห็นด้วย 3. ไม่แน่ใจ 4. ไม่เห็นด้วย 5. ไม่เห็นด้วยที่สุด
1.2 ท่านจะดำเนินการตามข้อความที่ปรากฏในอีเมล หากส่งมาจากบริษัทที่ติดต่อประจำและสามารถระบุข้อมูลเบื้องต้นของท่านได้ถูกต้อง	
1.3 ท่านรู้สึกตื่นตระหนกหากได้รับการติดต่อจากหน่วยงานด้านความมั่นคงของประเทศ	
1.4 ท่านได้รับการติดต่อจากกรมสรรพากร ผ่านช่องทางแชทให้ท่านเสียภาษี ท่านจะรีบดำเนินการทันที	
2. การสร้างความน่าเชื่อถือ	
2.1 ท่านจะเชื่อถือข้อความในสื่อออนไลน์ หากเขียนด้วยภาษาทางการ	1. เห็นด้วยที่สุด 2. เห็นด้วย 3. ไม่แน่ใจ 4. ไม่เห็นด้วย 5. ไม่เห็นด้วยที่สุด
2.2 ท่านจะเชื่อถือการรีวิว หากเนื้อหาเป็นไปในทิศทางเดียวกันจำนวนมาก	
2.3 ท่านจะเชื่อถือบุคคลที่อ้างตนว่าเป็นเจ้าหน้าที่ของรัฐจากโปรไฟล์โซเชียลและภาพถ่าย	
2.4 ท่านเชื่อถือลิงก์ที่นามสกุล (โดเมน) ไม่รู้จัก หากส่งมาโดยคนรู้จัก	

ตารางที่ ค.2 การจำแนกค่าองค์ประกอบที่เกี่ยวข้องกับปัจจัยการสื่อสาร (ต่อ)

รายการคำถาม	ค่าองค์ประกอบ
เนื้อหาสาร (Messages)	
3. กระตุ้นความสนใจ	
3.1 ท่านรู้สึกกังวลทุกครั้งเมื่อเห็นคำว่า “เฟซโดนแฮ็ก”, “กู้คืนบัญชีโดยด่วน” ในอีเมล	1. เห็นด้วยที่สุด 2. เห็นด้วย 3. ไม่แน่ใจ 4. ไม่เห็นด้วย 5. ไม่เห็นด้วยที่สุด
3.2 ท่านรู้สึกตื่นเต้นเมื่อได้รับข้อความว่า “ท่านเป็นผู้โชคดี”	
3.3 ท่านจะไม่ส่งต่อข้อมูลเหล่านั้น หากพบว่าเป็นข่าวปลอม แชร์ลูกโซ่*	
3.4 ท่านมักจะให้ความสนใจกับข้อความที่จำกัดระยะเวลา เช่น “ดูด่วนก่อนโดนลบ”	
4. กระตุ้นความต้องการ	
4.1 ท่านจะบอกหมายเลขบัญชีให้กับหน่วยงานที่บอกว่าจะโอนเงินรางวัลพิเศษให้	1. เห็นด้วยที่สุด 2. เห็นด้วย 3. ไม่แน่ใจ 4. ไม่เห็นด้วย 5. ไม่เห็นด้วยที่สุด
4.2 ท่านยินดีบอกข้อมูลให้กับทนายอาสาบนโลกออนไลน์ที่บอกว่าจะช่วยให้ท่านไม่ถูกดำเนินคดี	
4.3 ท่านยินดีโอนค่ามัดจำให้กับเว็บไซต์ที่ระบุว่าจะทำให้ท่านได้สินค้าราคาถูกกว่าท้องตลาด	
4.4 ท่านมักจะคลิกลิงก์เพื่อทำความสะอาดกล่องข้อความตามคำแนะนำที่ระบุไว้ในอีเมล	

ตารางที่ ค.2 การจำแนกค่าองค์ประกอบที่เกี่ยวข้องกับปัจจัยการสื่อสาร (ต่อ)

รายการคำถาม	ค่าองค์ประกอบ
5. สร้างความคาดหวัง	
5.1 ท่านรู้สึกดีใจหากได้รับข้อความว่า “ได้รับเงินช่วยเหลือสวัสดิการจากภาครัฐ”	1. เห็นด้วยที่สุด 2. เห็นด้วย 3. ไม่แน่ใจ 4. ไม่เห็นด้วย 5. ไม่เห็นด้วยที่สุด
5.2 ท่านยินดีชำระค่าธรรมเนียม เพื่อรับเงินสกุลดิจิทัลที่มีมูลค่าสูงจากต่างประเทศ	
5.3 ท่านพิจารณาอย่างถี่ถ้วนเกี่ยวกับส่วนลดที่ได้จากการร่วมกิจกรรม*	
5.4 ท่านจะตรวจสอบข้อมูลจากหน่วยงานต้นสังกัดก่อนทำธุรกรรมด้วยเสมอ*	
ผู้รับสาร (Receiver)	
6. ความกลัว	
6.1 ท่านรู้สึกกลัวข้อมูลในเครื่องคอมพิวเตอร์อาจถูกขโมยจึงดำเนินการสำรองข้อมูลอย่างสม่ำเสมอ	1. เห็นด้วยที่สุด 2. เห็นด้วย 3. ไม่แน่ใจ 4. ไม่เห็นด้วย 5. ไม่เห็นด้วยที่สุด
6.2 ท่านรู้สึกกลัว เมื่อมีคนรู้จักทักว่าเดือดร้อนต้องการขอยืมเงิน	
6.3 ท่านรู้สึกกลัว เมื่อมีผู้อ้างว่าครอบครองภาพลับของท่านไว้	
6.4 ท่านรู้สึกกลัวหากได้รับข้อความว่า “บัญชีของท่านเข้าข่ายการฟอกเงิน”	
6.5 ท่านรู้สึกกลัวหากได้รับข้อความว่า “เป็นหนี้บัตรเครดิตในจำนวนที่สูง”	

ตารางที่ ค.2 การจำแนกค่าองค์ประกอบที่เกี่ยวข้องกับปัจจัยการสื่อสาร (ต่อ)

รายการคำถาม	ค่าองค์ประกอบ
7. ความโลภ	
7.1 ท่านให้ข้อมูลส่วนตัว อาทิ ชื่อ ที่อยู่ เบอร์โทรศัพท์ กับเว็บไซต์ที่สัญญาว่าจะให้รางวัลท่าน	1. เห็นด้วยที่สุด 2. เห็นด้วย 3. ไม่แน่ใจ 4. ไม่เห็นด้วย 5. ไม่เห็นด้วยที่สุด
7.2 ท่านจะกดรหัสสั้น (USSD) เพื่อลุ้นรับรางวัลใหญ่กับหน่วยงานที่ท่านไม่รู้จัก	
7.3 ท่านจะกรอกข้อมูลบนแอปฯ ที่ไม่รู้จัก หากแอปฯ นั้นระบุว่าจะมอบส่วนลดของร้านค้าชื่อดังให้	
7.4 ท่านรู้สึกพิเศษ เมื่อได้รับข้อความที่ระบุว่ามอบสิทธิพิเศษให้เฉพาะคุณเท่านั้น	
8. ความอยากรู้อยากเห็น	
8.1 ท่านเปิดไฟล์แนบในอีเมลที่ได้รับจากบุคคลที่ไม่รู้จัก	1. เห็นด้วยที่สุด 2. เห็นด้วย 3. ไม่แน่ใจ 4. ไม่เห็นด้วย 5. ไม่เห็นด้วยที่สุด
8.2 ท่านคลิกลิงก์ในแอปสนทนาซึ่งได้รับจากบุคคลที่ไม่รู้จัก	
8.3 ท่านดาวน์โหลดไฟล์ที่ไม่เกี่ยวข้องกับงานในเวลางาน	
8.4 ท่านกดยอมรับข้อตกลงการใช้งานเว็บไซต์ทันที โดยไม่ได้อ่านข้อมูลทั้งหมด	
9. การตัดสินใจอย่างไม่มีเหตุผล	
9.1 ท่านใช้อีเมลของบริษัทเพื่อลงทะเบียนในเว็บไซต์ต่าง ๆ	1. เห็นด้วยที่สุด 2. เห็นด้วย 3. ไม่แน่ใจ 4. ไม่เห็นด้วย 5. ไม่เห็นด้วยที่สุด
9.2 ท่านเขียนหรือบันทึกรหัสผ่าน (Password) ไว้ในสถานที่ที่ผู้อื่นพบได้ง่าย	
9.3 ท่านทดลองคลิกลิงก์ไปเรื่อย ๆ เพื่อค้นหาไฟล์ที่ท่านต้องการดาวน์โหลด	

ภาคผนวก ค

แบบสอบถามเพื่อการวิจัย (ฉบับร่าง)

แบบสอบถามการสื่อสารที่มีความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล

คำชี้แจง

แบบสอบถามฉบับนี้เป็นส่วนหนึ่งของการวิจัย เรื่อง การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล โดยมีวัตถุประสงค์เพื่อพัฒนาแบบจำลองความสัมพันธ์ของปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัลด้วยเทคนิคเหมืองข้อมูล ซึ่งแบบสอบถามแบ่งออกเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 ความหมายของการถูกล่อลวงบนสื่อดิจิทัล

ส่วนที่ 2 คำถามคัดกรองผู้ตอบแบบสอบถาม

ส่วนที่ 3 ปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

ส่วนที่ 1 ความหมายของการถูกล่อลวงบนสื่อดิจิทัล

การล่อลวงบนสื่อดิจิทัลคืออะไร ?

การล่อลวงบนสื่อดิจิทัล นับได้ว่าเป็นหนึ่งในอาชญากรรมคอมพิวเตอร์ประเภทการฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ที่มีวัตถุประสงค์ในการลักลอบขโมยข้อมูลสำคัญของผู้เสียหาย เช่น ชื่อผู้ใช้ รหัสผ่าน รหัสบัตรเครดิต หรือข้อมูลสำหรับทำธุรกรรมทางอิเล็กทรอนิกส์

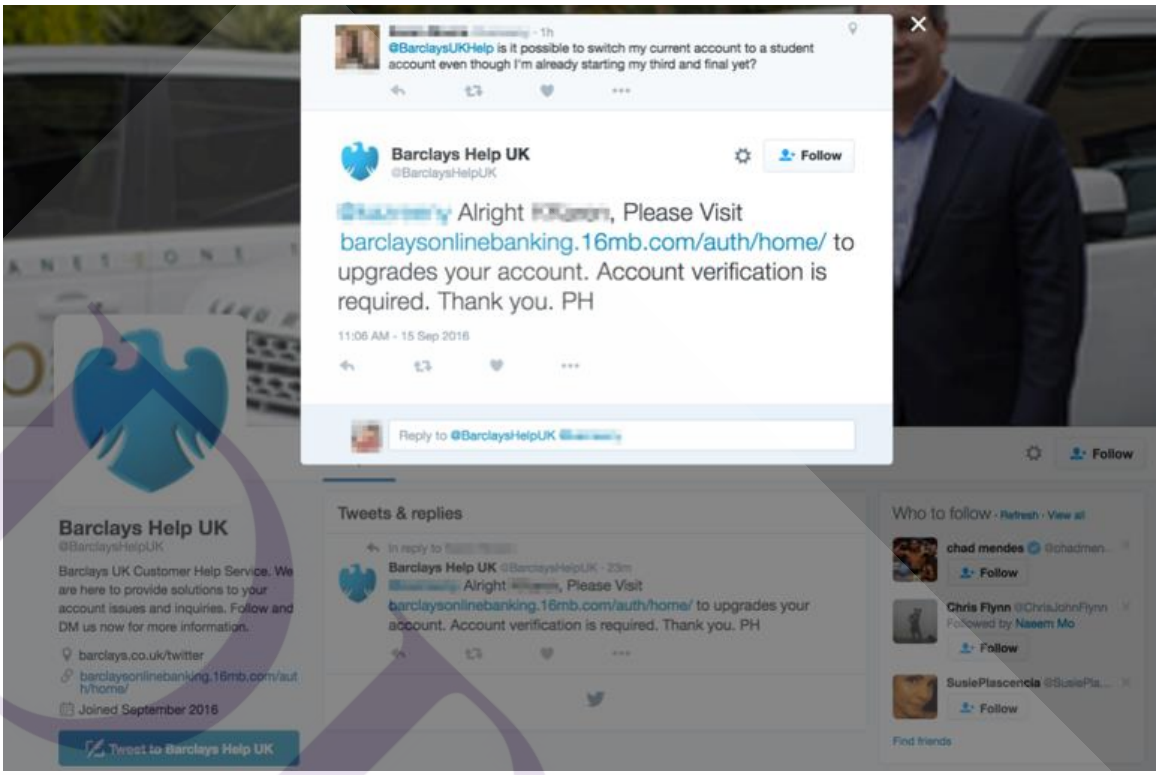
โดยส่วนใหญ่นิยมโจมตีโดยใช้วิธีการ ฟิชชิ่ง (Phishing) ปลอมแปลงเป็นระบบจากองค์กรหรือหน่วยงานที่น่าเชื่อถือเพื่อหลอกขอข้อมูลสำคัญจากเหยื่อ โดยปกติจะพบเห็นการแพร่กระจายของฟิชชิ่งผ่านอีเมลเป็นหลัก แต่ในปัจจุบันได้มีการกระจายไปยังช่องทางอื่น ๆ อาทิ ส่งข้อความผ่านแชทเฟซบุ๊ก ส่งผ่าน SMS รวมถึงโทรหลอกลวงผ่านโทรศัพท์

ตัวอย่างการล่อลวงบนสื่อดิจิทัล

คำชี้แจง : ปลอมเป็นผู้ให้บริการโทรศัพท์มือถือเพื่อให้เหยื่อกดติดตั้งแอปพลิเคชันอันตรายลงบนเครื่อง

ตัวอย่างการล่อลวงบนสื่อดิจิทัล ผ่านทางโซเชียลมีเดีย

คำชี้แจง : ลิงก์ปลอมจากโซเชียลมีเดียทวิตเตอร์



ส่วนที่ 2 คำถามคัดกรองผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงตามข้อมูลเบื้องต้นของผู้ตอบแบบสอบถาม

1. ท่านมีอายุอยู่ในช่วงใดต่อไปนี้

   [ ] อายุ 18 – 36 ปี [ ] อายุไม่ตรงตามเกณฑ์ดังกล่าว (จบการตอบแบบสอบถาม)

2. ท่านมีประสบการณ์การใช้งานอินเทอร์เน็ตมาเป็นระยะเวลาเท่าไร

   [ ] 5 ปี หรือมากกว่า [ ] น้อยกว่า 5 ปี (จบการตอบแบบสอบถาม)

ส่วนที่ 3 ปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงตามข้อมูลเบื้องต้นของผู้ตอบแบบสอบถาม

ตอนที่ 1. ปัจจัยทางประชากรศาสตร์

1. เพศ

[ ] ชาย [ ] หญิง [ ] กลุ่มบุคคลที่มีความหลากหลายทางเพศ

2. อายุ

[ ] 18 ปี [ ] 19 ปี [ ] 20 ปี [ ] 21 ปี

[ ] 22 ปี [ ] 23 ปี [ ] 24 ปี [ ] 25 ปี

[ ] 26 ปี [ ] 27 ปี [ ] 28 ปี [ ] 29 ปี

[ ] 30 ปี [ ] 31 ปี [ ] 32 ปี [ ] 33 ปี

[ ] 34 ปี [ ] 35 ปี [ ] 36 ปี

3. ระดับการศึกษา

[ ] ต่ำกว่าปริญญาตรี [ ] ปริญญาตรี [ ] ปริญญาโท [ ] ปริญญาเอก

4. อาชีพ

[ ] นักเรียน/นักศึกษา [ ] ข้าราชการ/พนักงานรัฐวิสาหกิจ

[ ] พนักงานบริษัทเอกชน [ ] ประกอบธุรกิจส่วนตัว/เจ้าของกิจการ

[ ] แม่บ้าน/พ่อบ้าน [ ] อื่น ๆ โปรดระบุ.....

5. รายได้เฉลี่ยต่อเดือน

[ ] 5,000 บาท หรือต่ำกว่า [ ] 5,001 - 10,000 บาท

[ ] 10,001 - 15,000 บาท [ ] 15,001 – 20,000 บาท

[ ] 20,001 - 25,000 บาท [ ] 25,001 – 30,000 บาท

[ ] มากกว่า 30,000 บาท

ตอนที่ 2. ปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงตามข้อมูลเบื้องต้นของผู้ตอบแบบสอบถาม

โดย **5 = ทำเป็นประจำ** **4 = ทำค่อนข้างบ่อย** **3 = ทำบ้างไม่ทำบ้าง**

2 = นาน ๆ ทำที **1 = ไม่ทำเลย**

รายการคำถาม	ระดับความบ่อยครั้ง				
	5	**4**	**3**	**2**	**1**
1. ผู้ส่งสาร (Sender)					
1.1 เมื่อท่านได้รับโทรศัพท์จากเลขหมายที่ท่านไม่รู้จัก ร้องขอข้อมูลส่วนตัวเพื่อยืนยันสิทธิ์รับรางวัลใหญ่ ท่านจะให้ข้อมูลเหล่านั้น					
1.2 เมื่อท่านได้รับอีเมลที่ส่งออกจากองค์กรที่น่าเชื่อถือ ท่านจะอ่านรายละเอียดเนื้อหาทั้งหมดก่อนกดลิงก์ในอีเมลดังกล่าว					
1.3 เมื่อท่านได้รับแชทจากเฟซบุ๊ก ร้องขอชื่อผู้ใช้และรหัสผ่าน โดยอ้างเหตุผลว่าท่านทำผิดกฎแพลตฟอร์ม ท่านจะให้ข้อมูลเหล่านั้น					
1.4 เมื่อท่านได้รับการติดต่อจากธนาคาร เรื่องพบการซื้อสินค้าผ่านบัญชีของท่าน โดยที่ท่านไม่ได้ซื้อสินค้าเหล่านั้น ท่านจะกดลิงก์ในอีเมลเพื่อขอเงินคืน					
1.5 เมื่อท่านได้รับการติดต่อจากหน่วยงานรัฐแจ้งว่าท่านทำผิดกฎหมายด้านภาษี และขอให้ท่านโอนเงินดังกล่าวไปยังบัญชีหนึ่ง ท่านจะรีบดำเนินการตามนั้นทันที					

รายการคำถาม	ระดับความบ่อยครั้ง				
	5	4	3	2	1
2. สาร (Messages)					
2.1 เมื่อท่านสมัครสมาชิกบนแพลตฟอร์มออนไลน์ ท่านจะกดยอมรับเงื่อนไขการสมัครโดยไม่ได้กดอ่านรายละเอียด					
2.2 เมื่อท่านได้รับลิงก์สำหรับดาวน์โหลดไฟล์หรือวิดีโอ ท่านจะกดที่ลิงก์เหล่านั้นโดยทันที					
2.3 เมื่อท่านได้รับข้อความว่าเป็นผู้โชคดี ท่านจะคลิกลิงก์และให้รายละเอียดที่อยู่เพื่อยืนยันการรับรางวัล					
2.4 เมื่อท่านได้รับแชทจากเพื่อนสนิททักมาขอยืมเงิน ท่านจะขอยืนยันตัวตนเพื่อนและเช็กเลขบัญชีปลายทางก่อนเสมอ					
2.5 เมื่อท่านได้รับเลือกให้เป็นคนกลุ่มแรกที่ได้ใช้งานผลิตภัณฑ์ใหม่จากต่างประเทศฟรี แต่มีค่าส่ง ท่านจะโอนเงินค่าส่งของให้กับเจ้าของผลิตภัณฑ์นั้น					
3. ผู้รับสาร (Receiver)					
3.1 เมื่อท่านสมัครสมาชิกเว็บไซต์ออนไลน์ ท่านจะเลือกใช้รหัสผ่านชุดเดียวกัน					
3.2 เมื่อท่านได้รับข้อความแจ้งเตือนเกี่ยวกับการกระทำผิดกฎหมาย ท่านจะพิจารณาถี่ถ้วนก่อนดำเนินการ					

รายการคำถาม	ระดับความบ่อยครั้ง				
	5	4	3	2	1
3. ผู้รับสาร (Receiver) (ต่อ)					
3.3 เมื่อท่านได้รับข้อความเชิญชวนทำแบบสอบถามลุ้นรับรางวัลโทรศัพท์รุ่นใหม่ ท่านจะทำแบบสอบถาม และทำตามขั้นตอนทั้งหมดที่เว็บไซต์ระบุไว้					
3.4 เมื่อท่านได้รับการเชิญชวนให้เข้ากลุ่มลับ ท่านจะกดยอมรับการเชิญชวนทันที					
3.5 เมื่อท่านอ่านเงื่อนไขการใช้งานแอปพลิเคชันไม่เข้าใจ ท่านจะปล่อยผ่านและกดยอมรับข้อตกลงทันที					

ตอนที่ 3. ข้อเสนอแนะเพิ่มเติม

ข้อเสนอแนะเพิ่มเติมเกี่ยวกับปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

……

……

……

****

ขอบคุณครับ

ภาคผนวก ง

แบบสอบถามเพื่อการวิจัย

แบบสอบถามการสื่อสารที่มีความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล

คำชี้แจง

แบบสอบถามฉบับนี้เป็นส่วนหนึ่งของการวิจัย เรื่อง การพัฒนาแบบจำลองด้านการสื่อสารเพื่อพยากรณ์ความเสี่ยงต่อการถูกล่อลวงบนสื่อดิจิทัล โดยใช้เทคนิคเหมืองข้อมูล โดยมีวัตถุประสงค์เพื่อพัฒนาแบบจำลองความสัมพันธ์ของปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัลด้วยเทคนิคเหมืองข้อมูล ซึ่งแบบสอบถามแบ่งออกเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 ความหมายของการถูกล่อลวงบนสื่อดิจิทัล

ส่วนที่ 2 คำถามคัดกรองผู้ตอบแบบสอบถาม

ส่วนที่ 3 ปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

ส่วนที่ 1 ความหมายของการถูกล่อลวงบนสื่อดิจิทัล

การล่อลวงบนสื่อดิจิทัลคืออะไร ?

การล่อลวงบนสื่อดิจิทัล นับได้ว่าเป็นหนึ่งในอาชญากรรมคอมพิวเตอร์ประเภทการฉ้อฉล ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ที่มีวัตถุประสงค์ในการลักลอบขโมยข้อมูลสำคัญของผู้เสียหาย เช่น ชื่อผู้ใช้ รหัสผ่าน รหัสบัตรเครดิต หรือข้อมูลสำหรับทำธุรกรรมทางอิเล็กทรอนิกส์

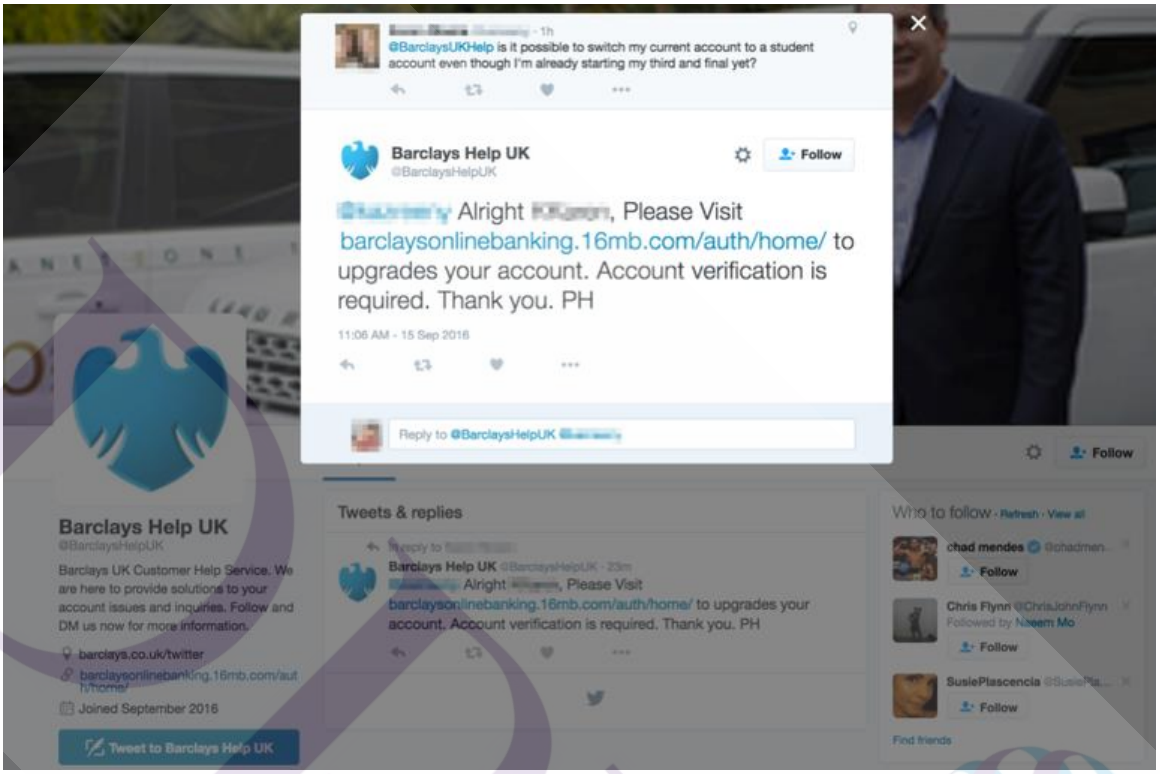
โดยส่วนใหญ่นิยมโจมตีโดยใช้วิธีการ ฟิชชิ่ง (Phishing) ปลอมแปลงเป็นระบบจากองค์กรหรือหน่วยงานที่น่าเชื่อถือเพื่อหลอกขอข้อมูลสำคัญจากเหยื่อ โดยปกติจะพบเห็นการแพร่กระจายของฟิชชิ่งผ่านอีเมลเป็นหลัก แต่ในปัจจุบันได้มีการกระจายไปยังช่องทางอื่น ๆ อาทิ ส่งข้อความผ่านแชทเฟซบุ๊ก ส่งผ่าน SMS รวมถึงโทรหลอกลวงผ่านโทรศัพท์

ตัวอย่างการล่อลวงบนสื่อดิจิทัล

คำชี้แจง: ปลอมเป็นผู้ให้บริการโทรศัพท์มือถือเพื่อให้เหยื่อกดติดตั้งแอปพลิเคชันอันตรายลงบนเครื่อง

ตัวอย่างการล่อลวงบนสื่อดิจิทัล ผ่านทางโซเชียลมีเดีย

คำชี้แจง : ลิงก์ปลอมจากโซเชียลมีเดียทวิตเตอร์



ส่วนที่ 2 คำถามคัดกรองผู้ตอบแบบสอบถาม

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงตามข้อมูลเบื้องต้นของผู้ตอบแบบสอบถาม

1. ท่านมีอายุอยู่ในช่วงใดต่อไปนี้

   [ ] อายุ 18 – 36 ปี [ ] อายุไม่ตรงตามเกณฑ์ดังกล่าว (จบการตอบแบบสอบถาม)

2. ท่านมีประสบการณ์การใช้งานอินเทอร์เน็ตมาเป็นระยะเวลาเท่าไร

   [ ] 5 ปี หรือมากกว่า [ ] น้อยกว่า 5 ปี (จบการตอบแบบสอบถาม)

ส่วนที่ 3 ปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงตามข้อมูลเบื้องต้นของผู้ตอบแบบสอบถาม

ตอนที่ 1. ปัจจัยทางประชากรศาสตร์

1. เพศ

[ ] ชาย [ ] หญิง [ ] กลุ่มบุคคลที่มีความหลากหลายทางเพศ

2. อายุ

[ ] 18-21 ปี [ ] 22-25 ปี [ ] 26-29 ปี [ ] 30-33 ปี

[ ] 34-36 ปี

3. ระดับการศึกษา

[ ] ต่ำกว่าปริญญาตรี [ ] ปริญญาตรี [ ] ปริญญาโท [ ] ปริญญาเอก

4. อาชีพ

[ ] นักเรียน/นักศึกษา [ ] ข้าราชการ/พนักงานรัฐวิสาหกิจ

[ ] พนักงานบริษัทเอกชน [ ] ประกอบธุรกิจส่วนตัว/เจ้าของกิจการ

[ ] แม่บ้าน/พ่อบ้าน [ ] อื่น ๆ โปรดระบุ.....

5. รายได้เฉลี่ยต่อเดือน

[ ] 5,000 บาท หรือต่ำกว่า [ ] 5,001 - 10,000 บาท

[ ] 10,001 - 15,000 บาท [ ] 15,001 – 20,000 บาท

[ ] 20,001 - 25,000 บาท [ ] 25,001 – 30,000 บาท

[ ] มากกว่า 30,000 บาท

ตอนที่ 2. ปัจจัยการสื่อสารที่มีผลต่อการถูกล่อลวงบนสื่อดิจิทัล

<u>คำชี้แจง</u> โปรดทำเครื่องหมาย ✓ ลงในช่องที่ตรงตามข้อมูลเบื้องต้นของผู้ตอบแบบสอบถาม

โดย **5 = เห็นด้วยที่สุด** **4 = เห็นด้วย** **3 = ไม่แน่ใจ**

2 = ไม่เห็นด้วย **1 = ไม่เห็นด้วยที่สุด**

รายการคำถาม	ระดับความคิดเห็น				
	5	**4**	**3**	**2**	**1**
ผู้ส่งสาร (Sender)					
1. อ้างเป็นบุคคลสำคัญ					
1.1 ท่านเชื่อถือข้อมูลเหล่านั้นทันที หากส่งมาจากบุคคลที่รู้จัก					
1.2 ท่านจะดำเนินการตามข้อความที่ปรากฏในอีเมล หากส่งมาจากบริษัทที่ติดต่อประจำและสามารถระบุข้อมูลเบื้องต้นของท่านได้ถูกต้อง					
1.3 ท่านรู้สึกตื่นตระหนกหากได้รับการติดต่อจากหน่วยงานด้านความมั่นคงของประเทศ					
1.4 ท่านได้รับการติดต่อจากกรมสรรพากรผ่านช่องทางแชทให้ท่านเสียภาษี ท่านจะรีบดำเนินการทันที					
2. การสร้างความน่าเชื่อถือ					
2.1 ท่านจะเชื่อถือข้อความในสื่อออนไลน์ หากเขียนด้วยภาษาทางการ					
2.2 ท่านจะเชื่อถือการรีวิว หากเนื้อหาเป็นไปในทิศทางเดียวกันจำนวนมาก					
2.3 ท่านจะเชื่อถือบุคคลที่อ้างตนว่าเป็นเจ้าหน้าที่ของรัฐจากโปรไฟล์โซเชียลและภาพถ่าย					

รายการคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
2. การสร้างความน่าเชื่อถือ (ต่อ)					
2.4 ท่านเชื่อถือลิงก์ที่นามสกุล (โดเมน) ไม่รู้จัก หากส่งมาโดยคนรู้จัก					
เนื้อหาสาร (Messages)					
3. กระตุ้นความสนใจ					
3.1 ท่านรู้สึกกังวลทุกครั้งเมื่อเห็นคำว่า “เฟซโดนแฮ็ก”, “กู้คืนบัญชีโดยด่วน” ในอีเมล					
3.2 ท่านรู้สึกตื่นเต้นเมื่อได้รับข้อความว่า “ท่านเป็นผู้โชคดี”					
3.3 ท่านจะไม่ส่งต่อข้อมูลเหล่านั้น หากพบว่าเป็นข่าวปลอม แชร์ลูกโซ่*					
3.4 ท่านมักจะให้ความสนใจกับข้อความที่จำกัดระยะเวลา เช่น “ดูด่วนก่อนโดนลบ”					
4. กระตุ้นความต้องการ					
4.1 ท่านจะบอกหมายเลขบัญชีให้กับหน่วยงานที่บอกว่าจะโอนเงินรางวัลพิเศษให้					
4.2 ท่านยินดีบอกข้อมูลให้กับทนายอาสาบนโลกออนไลน์ที่บอกว่าจะช่วยให้ท่านไม่ถูกดำเนินคดี					
4.3 ท่านยินดีโอนค่ามัดจำให้กับเว็บไซต์ที่ระบุว่าจะทำให้ท่านได้สินค้าราคาถูกกว่าท้องตลาด					
4.4 ท่านมักจะคลิกลิงก์เพื่อทำความสะอาดกล่องข้อความ ตามคำแนะนำที่ระบุไว้ในอีเมล					

รายการคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
5. สร้างความคาดหวัง					
5.1 ท่านรู้สึกดีใจหากได้รับข้อความว่า “ได้รับเงินช่วยเหลือสวัสดิการจากภาครัฐ”					
5.2 ท่านยินดีชำระค่าธรรมเนียม เพื่อรับเงินสกุลดิจิทัลที่มีมูลค่าสูงจากต่างประเทศ					
5.3 ท่านพิจารณาอย่างถี่ถ้วนเกี่ยวกับส่วนลดที่ได้จากการร่วมกิจกรรม*					
5.4 ท่านจะตรวจสอบข้อมูลจากหน่วยงานต้นสังกัดก่อนทำธุรกรรมด้วยเสมอ*					
ผู้รับสาร (Messages)					
6. ความกลัว					
6.1 ท่านรู้สึกกลัวข้อมูลในเครื่องคอมพิวเตอร์อาจถูกขโมยจึงดำเนินการสำรองข้อมูลอย่างสม่ำเสมอ					
6.2 ท่านรู้สึกกลัว เมื่อมีคนรู้จักทักว่าเดือดร้อนต้องการขอยืมเงิน					
6.3 ท่านรู้สึกกลัว เมื่อมีผู้อ้างว่าครอบครองภาพลับของท่านไว้					
6.4 ท่านรู้สึกกลัวหากได้รับข้อความว่า “บัญชีของท่านเข้าข่ายการฟอกเงิน”					
6.5 ท่านรู้สึกกลัวหากได้รับข้อความว่า “เป็นหนี้บัตรเครดิตในจำนวนที่สูง”					

รายการคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
7. ความโลภ					
7.1 ท่านให้ข้อมูลส่วนตัว อาทิ ชื่อ ที่อยู่ เบอร์โทรศัพท์ กับเว็บไซต์ที่สัญญาว่าจะให้รางวัลท่าน					
7.2 ท่านจะกดรหัสสั้น (USSD) เพื่อลุ้นรับรางวัลใหญ่กับหน่วยงานที่ท่านไม่รู้จัก					
7.3 ท่านจะกรอกข้อมูลบนแอปฯ ที่ไม่รู้จัก หากแอปฯ นั้นระบุว่าจะมอบส่วนลดของร้านค้าชื่อดังให้					
7.4 ท่านรู้สึกพิเศษ เมื่อได้รับข้อความที่ระบุว่ามอบสิทธิพิเศษให้เฉพาะคุณเท่านั้น					
8. ความอยากรู้อยากเห็น					
8.1 ท่านเปิดไฟล์แนบในอีเมลที่ได้รับจากบุคคลที่ไม่รู้จัก					
8.2 ท่านคลิกลิงก์ในแอปสนทนาซึ่งได้รับจากบุคคลที่ไม่รู้จัก					
8.3 ท่านดาวน์โหลดไฟล์ที่ไม่เกี่ยวข้องกับงานในเวลางาน					
8.4 ท่านกดยอมรับข้อตกลงการใช้งานเว็บไซต์ทันที โดยไม่ได้อ่านข้อมูลทั้งหมด					
9. การตัดสินใจอย่างไม่มีเหตุผล					
9.1 ท่านใช้อีเมลของบริษัทเพื่อลงทะเบียนในเว็บไซต์ต่าง ๆ					

รายการคำถาม	ระดับความคิดเห็น				
	5	4	3	2	1
9. การตัดสินใจอย่างไม่มีเหตุผล (ต่อ)					
9.2 ท่านเขียนหรือบันทึกรหัสผ่าน (Password) ไว้ในสถานที่ที่ผู้อื่นพบได้ง่าย					
9.3 ท่านทดลองคลิกลิงก์ไปเรื่อย ๆ เพื่อค้นหาไฟล์ที่ท่านต้องการดาวน์โหลด					

ตอนที่ 3. ข้อเสนอแนะเพิ่มเติม

ข้อเสนอแนะเพิ่มเติม

.....

.....

.....

****

ขอบคุณครับ

ภาคผนวก จ

การวิเคราะห์ข้อมูล

ตารางที่ ฉ.1 วิเคราะห์คุณภาพแบบสอบถามด้านคำถามคัดกรอง

รายการคำถาม	ผู้ทรงคุณวุฒิ			$\bar{X}$	แปลผล
	1	2	3		
1. ท่านมีอายุอยู่ในช่วงใดต่อไปนี้ [ ] อายุ 18 – 36 ปี [ ] อายุไม่ตรงตามเกณฑ์ดังกล่าว (จบการตอบแบบสอบถาม)	1	1	1	1	ใช้ได้
2. ท่านมีประสบการณ์การใช้งานอินเทอร์เน็ตมาเป็นระยะเวลาเท่าไร [ ] 5 ปี หรือมากกว่า [ ] น้อยกว่า 5 ปี (จบการตอบแบบสอบถาม)	1	1	1	1	ใช้ได้

ตารางที่ ฉ.2 วิเคราะห์คุณภาพแบบสอบถามด้านปัจจัยด้านประชากรศาสตร์

รายการคำถาม	ผู้ทรงคุณวุฒิ			$\bar{X}$	แปลผล
	1	2	3		
1. เพศ [ ] ชาย [ ] หญิง [ ] กลุ่มบุคคลที่มีความหลากหลายทางเพศ	1	1	1	1	ใช้ได้
2. อายุ [ ] 18 - 21 ปี [ ] 22 - 25 ปี [ ] 26 - 29 ปี [ ] 30 - 33 ปี [ ] 34 - 36 ปี	1	1	1	1	ใช้ได้
3. ระดับการศึกษา [ ] ต่ำกว่าปริญญาตรี [ ] ปริญญาตรี [ ] ปริญญาโท [ ] ปริญญาเอก	1	1	1	1	ใช้ได้
4. อาชีพ [ ] นักเรียน/นักศึกษา [ ] ข้าราชการ/พนักงานรัฐวิสาหกิจ [ ] พนักงานบริษัทเอกชน [ ] ประกอบธุรกิจส่วนตัว/เจ้าของกิจการ [ ] แม่บ้าน/พ่อบ้าน [ ] อื่น ๆ โปรดระบุ……..	0	1	1	0.67	ใช้ได้

ตารางที่ ฉ.2 วิเคราะห์คุณภาพแบบสอบถามด้านปัจจัยด้านประชากรศาสตร์ (ต่อ)

5. รายได้เฉลี่ยต่อเดือน [ ] 5,000 บาท หรือต่ำกว่า [ ] 5,001 - 10,000 บาท [ ] 10,001 - 15,000 บาท [ ] 15,001 – 20,000 บาท [ ] 20,001 - 25,000 บาท [ ] 25,001 – 30,000 บาท [ ] มากกว่า 30,000 บาท	1	0	1	0.67	ใช้ได้

ตารางที่ ฉ.3 วิเคราะห์คุณภาพแบบสอบถามด้านปัจจัยด้านการสื่อสาร

รายการคำถาม	ผู้ทรงคุณวุฒิ			$\bar{X}$	แปลผล
	1	2	3		
ผู้ส่งสาร (Sender)					
1. อ้างเป็นบุคคลสำคัญ					
1.1 ท่านเชื่อถือข้อมูลเหล่านั้นทันที หากส่งมาจากบุคคลที่รู้จัก	1	1	1	1	ใช้ได้
1.2 ท่านจะดำเนินการตามข้อความที่ปรากฏในอีเมลหากส่งมาจากบริษัทที่ติดต่อประจำและสามารถระบุข้อมูลเบื้องต้นของท่านได้ถูกต้อง	1	1	1	1	ใช้ได้
1.3 ท่านรู้สึกตื่นตระหนกหากได้รับการติดต่อจากหน่วยงานด้านความมั่นคงของประเทศ	1	1	1	1	ใช้ได้
1.4 ท่านได้รับการติดต่อจากกรมสรรพากร ผ่านช่องทางแชทให้ท่านเสียภาษี ท่านจะรีบดำเนินการทันที	1	1	1	1	ใช้ได้
2. การสร้างความน่าเชื่อถือ					
2.1 ท่านจะเชื่อถือข้อความในสื่อออนไลน์ หากเขียนด้วยภาษาทางการ	1	1	1	1	ใช้ได้
2.2 ท่านจะเชื่อถือการรีวิว หากเนื้อหาเป็นไปในทิศทางเดียวกันจำนวนมาก	1	1	1	1	ใช้ได้
2.3 ท่านจะเชื่อถือบุคคลที่อ้างตนว่าเป็นเจ้าหน้าที่ของรัฐจากโปรไฟล์โซเชียลและภาพถ่าย	1	1	1	1	ใช้ได้
2.4 ท่านเชื่อถือลิงก์ที่นามสกุล (โดเมน) ไม่รู้จัก หากส่งมาโดยคนรู้จัก	0	1	1	0.67	ใช้ได้

ตารางที่ ฉ.3 วิเคราะห์คุณภาพแบบสอบถามด้านปัจจัยด้านการสื่อสาร (ต่อ)

รายการคำถาม	ผู้ทรงคุณวุฒิ			$\bar{X}$	แปลผล
	1	2	3		
เนื้อหาสาร (Messages)					
3. กระตุ้นความสนใจ					
3.1 ท่านรู้สึกกังวลทุกครั้งเมื่อเห็นคำว่า “เฟซโดนแฮ็ก”, “กู้คืนบัญชีโดยด่วน” ในอีเมล	1	1	0	0.67	ใช้ได้
3.2 ท่านรู้สึกตื่นเต้นเมื่อได้รับข้อความว่า “ท่านเป็นผู้โชคดี”	0	1	1	0.67	ใช้ได้
3.3 ท่านจะไม่ส่งต่อข้อมูลเหล่านั้น หากพบว่าเป็นข่าวปลอม แชร์ลูกโซ่*	1	1	1	1	ใช้ได้
3.4 ท่านมักจะให้ความสนใจกับข้อความที่จำกัดระยะเวลา เช่น “ดูด่วนก่อนโดนลบ”	0	1	1	0.67	ใช้ได้
4. กระตุ้นความต้องการ					
4.1 ท่านจะบอกหมายเลขบัญชีให้กับหน่วยงานที่บอกว่าจะโอนเงินรางวัลพิเศษให้	1	1	1	1	ใช้ได้
4.2 ท่านยินดีบอกข้อมูลให้กับทนายอาสาบนโลกออนไลน์ที่บอกว่าจะช่วยให้ท่านไม่ถูกดำเนินคดี	0	1	1	0.67	ใช้ได้
4.3 ท่านยินดีโอนค่ามัดจำให้กับเว็บไซต์ที่ระบุว่าจะทำให้ท่านได้สินค้าราคาถูกกว่าท้องตลาด	1	0	1	0.67	ใช้ได้
4.4 ท่านมักจะคลิกลิงก์เพื่อทำความสะอาดกล่องข้อความ ตามคำแนะนำที่ระบุไว้ในอีเมล	0	1	1	0.67	ใช้ได้

ตารางที่ ฉ.3 วิเคราะห์คุณภาพแบบสอบถามด้านปัจจัยด้านการสื่อสาร (ต่อ)

รายการคำถาม	ผู้ทรงคุณวุฒิ			$\bar{X}$	แปลผล
	1	2	3		
5. สร้างความคาดหวัง					
5.1 ท่านรู้สึกดีใจหากได้รับข้อความว่า “ได้รับเงินช่วยเหลือสวัสดิการจากภาครัฐ”	1	1	0	0.67	ใช้ได้
5.2 ท่านยินดีชำระค่าธรรมเนียม เพื่อรับเงินสกุลดิจิทัลที่มีมูลค่าสูงจากต่างประเทศ	0	1	1	0.67	ใช้ได้
5.3 ท่านพิจารณาอย่างถี่ถ้วนเกี่ยวกับส่วนลดที่ได้จากการร่วมกิจกรรม*	0	1	1	0.67	ใช้ได้
5.4 ท่านจะตรวจสอบข้อมูลจากหน่วยงานต้นสังกัดก่อนทำธุรกรรมด้วยเสมอ*	1	1	1	1	ใช้ได้
ผู้รับสาร (Receiver)					
6. ความกลัว					
6.1 ท่านรู้สึกกลัวข้อมูลในเครื่องคอมพิวเตอร์อาจถูกขโมยจึงดำเนินการสำรองข้อมูลอย่างสม่ำเสมอ	1	0	1	0.67	ใช้ได้
6.2 ท่านรู้สึกกลัว เมื่อมีคนรู้จักทักว่าเดือดร้อนต้องการขอยืมเงิน	1	1	1	1	ใช้ได้
6.3 ท่านรู้สึกกลัว เมื่อมีผู้อ้างว่าครอบครองภาพลับของท่านไว้	0	1	1	0.67	ใช้ได้
6.4 ท่านรู้สึกกลัวหากได้รับข้อความว่า “บัญชีของท่านเข้าข่ายการฟอกเงิน”	1	1	1	1	ใช้ได้
6.5 ท่านรู้สึกกลัวหากได้รับข้อความว่า “เป็นหนี้บัตรเครดิตในจำนวนที่สูง”	0	1	1	0.67	ใช้ได้

ตารางที่ ฉ.3 วิเคราะห์คุณภาพแบบสอบถามด้านปัจจัยด้านการสื่อสาร (ต่อ)

รายการคำถาม	ผู้ทรงคุณวุฒิ			$\bar{X}$	แปลผล
	1	2	3		
7. ความโลภ					
7.1 ท่านให้ข้อมูลส่วนตัว อาทิ ชื่อ ที่อยู่ เบอร์โทรศัพท์ กับเว็บไซต์ที่สัญญาว่าจะให้รางวัลท่าน	0	1	1	0.67	ใช้ได้
7.2 ท่านจะกดรหัสสั้น (USSD) เพื่อลุ้นรับรางวัลใหญ่กับหน่วยงานที่ท่านไม่รู้จัก	0	1	1	0.67	ใช้ได้
7.3 ท่านจะกรอกข้อมูลบนแอปฯ ที่ไม่รู้จัก หากแอปนั้นระบุว่าจะมอบส่วนลดของร้านค้าชื่อดังให้	1	1	1	1	ใช้ได้
7.4 ท่านรู้สึกพิเศษ เมื่อได้รับข้อความที่ระบุว่ามอบสิทธิพิเศษให้เฉพาะคุณเท่านั้น	1	1	1	1	ใช้ได้
8. ความอยากรู้อยากเห็น					
8.1 ท่านเปิดไฟล์แนบในอีเมลที่ได้รับจากบุคคลที่ไม่รู้จัก	1	0	1	0.67	ใช้ได้
8.2 ท่านคลิกลิงก์ในแอปสนทนาซึ่งได้รับจากบุคคลที่ไม่รู้จัก	1	1	1	1	ใช้ได้
8.3 ท่านดาวน์โหลดไฟล์ที่ไม่เกี่ยวข้องกับงานในเวลางาน	0	1	1	0.67	ใช้ได้
8.4 ท่านกดยอมรับข้อตกลงการใช้งานเว็บไซต์ทันทีโดยไม่ได้อ่านข้อมูลทั้งหมด	1	1	1	1	ใช้ได้

ตารางที่ ฉ.3 วิเคราะห์คุณภาพแบบสอบถามด้านปัจจัยด้านการสื่อสาร (ต่อ)

รายการคำถาม	ผู้ทรงคุณวุฒิ			$\bar{X}$	แปลผล
	1	2	3		
9. การตัดสินใจอย่างไม่มีเหตุผล					
9.1 ท่านใช้อีเมลของบริษัทเพื่อลงทะเบียนในเว็บไซต์ต่าง ๆ	0	1	1	0.67	ใช้ได้
9.2 ท่านเขียนหรือบันทึกรหัสผ่าน (Password) ไว้ในสถานที่ที่ผู้อื่นพบได้ง่าย	1	1	1	1	ใช้ได้
9.3 ท่านทดลองคลิกลิงก์ไปเรื่อย ๆ เพื่อค้นหาไฟล์ที่ท่านต้องการดาวน์โหลด	1	1	0	0.67	ใช้ได้

ภาคผนวก ฉ

กฎที่ได้จากการวิเคราะห์ด้วยต้นไม้ตัดสินใจ J48

M3 = Strongly Disagree

| R3 = Strongly Disagree

| | M9 = Strongly Disagree: Very Low Risk (88.0/2.0)

| | M9 = Disagree: Very Low Risk (25.0/2.0)

| | M9 = Confuse

| | | M6 = Strongly Disagree: Very Low Risk (5.0)

| | | M6 = Disagree: Low Risk (3.0)

| | | M6 = Confuse: Medium Risk (1.0)

| | | M6 = Agree: Medium Risk (0.0)

| | | M6 = Strongly Agree: High Risk (0.0)

| | M9 = Agree: Low Risk (2.0)

| | M9 = Strongly Agree: Medium Risk (0.0)

| R3 = Disagree

| | R2 = Strongly Disagree: Very Low Risk (27.0)

| | R2 = Disagree

| | | M8 = Strongly Disagree: Very Low Risk (21.0)

| | | M8 = Disagree: Low Risk (12.0)

| | | M8 = Confuse: Medium Risk (2.0)

| | | M8 = Agree: High Risk (0.0)

| | | M8 = Strongly Agree: Very High Risk (1.0)

| | R2 = Confuse: Low Risk (4.0)

| | R2 = Agree: Medium Risk (5.0/1.0)

| | R2 = Strongly Agree

| | | R15 = Strongly Disagree: Low Risk (4.0)

| | | R15 = Disagree: Low Risk (1.0)

| | | R15 = Confuse: Medium Risk (2.0)

| | | R15 = Agree: Medium Risk (0.0)

| | | R15 = Strongly Agree: High Risk (0.0)

| R3 = Confuse: Low Risk (5.0)

| R3 = Agree

| | M11 = Strongly Disagree: High Risk (50.0/10.0)

| | M11 = Disagree

| | | AGE = 18-21: Low Risk (4.0/1.0)

| | | AGE = 22-25

| | | | R5 = Strongly Disagree: Low Risk (2.0)

| | | | R5 = Disagree: Low Risk (4.0/1.0)

| | | | R5 = Confuse: Medium Risk (3.0)

| | | | R5 = Agree: Medium Risk (4.0)

| | | | R5 = Strongly Agree: High Risk (9.0/1.0)

| | | AGE = 26-29: Low Risk (4.0/1.0)

| | | AGE = 30-33: Medium Risk (0.0)

| | | AGE = 34-36: Medium Risk (1.0)

| | M11 = Confuse: Medium Risk (9.0/1.0)

| | M11 = Agree: Low Risk (1.0)

| | M11 = Strongly Agree: Low Risk (2.0)

| R3 = Strongly Agree

| | EDU = Below Bachelor

| | | R15 = Strongly Disagree: Low Risk (18.0/1.0)

| | | R15 = Disagree

| | | | M10 = Strongly Disagree

| | | | | S6 = Strongly Disagree: Low Risk (0.0)

| | | | | S6 = Disagree: Low Risk (1.0)

| | | | | S6 = Confuse: Low Risk (2.0)

| | | | | S6 = Agree: Medium Risk (0.0)

| | | | | S6 = Strongly Agree: High Risk (2.0)

| | | | M10 = Disagree: Low Risk (2.0)

| | | | M10 = Confuse: Medium Risk (5.0)

| | | | M10 = Agree: High Risk (2.0)

| | | | M10 = Strongly Agree: Very High Risk (0.0)

| | | R15 = Confuse: Medium Risk (4.0/2.0)

| | | R15 = Agree: Medium Risk (5.0)

| | | R15 = Strongly Agree: High Risk (1.0)

| | EDU = Bachelor: Medium Risk (170.0/22.0)

| | EDU = Master: Low Risk (41.0/4.0)

| | EDU = Doctor: Low Risk (0.0)

M3 = Disagree

| R3 = Strongly Disagree: Very Low Risk (52.0/2.0)

| R3 = Disagree: Low Risk (61.0)

| R3 = Confuse: Medium Risk (1.0)

| R3 = Agree

| | M8 = Strongly Disagree

| | | EDU = Below Bachelor: Low Risk (5.0)

| | | EDU = Bachelor: Medium Risk (4.0/1.0)

| | | EDU = Master: Low Risk (0.0)

| | | EDU = Doctor: Low Risk (0.0)

| | M8 = Disagree: Low Risk (11.0)

| | M8 = Confuse: Medium Risk (4.0)

| | M8 = Agree: High Risk (2.0/1.0)

| | M8 = Strongly Agree: Very High Risk (1.0)

| R3 = Strongly Agree

| | OCC = STD

| | | R12 = Strongly Disagree: Low Risk (3.0)

| | | R12 = Disagree: Low Risk (3.0)

| | | R12 = Confuse: Medium Risk (1.0)

| | | R12 = Agree: Medium Risk (2.0)

| | | R12 = Strongly Agree: High Risk (0.0)

| | OCC = INC: Medium Risk (31.0)

| | OCC = GOV: High Risk (7.0/1.0)

| | OCC = PRV: Medium Risk (6.0/1.0)

| | OCC = HOM: Low Risk (0.0)

| | OCC = ETC: Medium Risk (0.0)

M3 = Confuse

| AGE = 18-21

| | R1 = Strongly Disagree: High Risk (0.0)

| | R1 = Disagree: Medium Risk (0.0)

| | R1 = Confuse: Medium Risk (0.0)

| | R1 = Agree: Low Risk (2.0)

| | R1 = Strongly Agree: Low Risk (2.0/1.0)

| AGE = 22-25

| | M12 = Strongly Disagree: High Risk (10.0)

| | M12 = Disagree

| | | SEX = Male: Low Risk (2.0)

| | | SEX = Female: Medium Risk (2.0)

| | | SEX = LGBT: Low Risk (0.0)

| | M12 = Confuse: Medium Risk (0.0)

| | M12 = Agree: Very Low Risk (0.0)

| | M12 = Strongly Agree: Very Low Risk (0.0)

| AGE = 26-29: Low Risk (1.0)

| AGE = 30-33: Medium Risk (0.0)

| AGE = 34-36: Medium Risk (1.0)

M3 = Agree

| R4 = Strongly Disagree: Very Low Risk (0.0)

| R4 = Disagree: Low Risk (1.0)

| R4 = Confuse: Medium Risk (3.0)

| R4 = Agree: Very High Risk (64.0/2.0)

| R4 = Strongly Agree: Very High Risk (84.0)

M3 = Strongly Agree: Very Low Risk (191.0/3.0)

ประวัติผู้เขียน

ชื่อ-สกุล	นายดำรงศักดิ์ สัตบุตร
วัน-เดือน-ปีเกิด	10 สิงหาคม 2539
สถานที่เกิด	กรุงเทพมหานคร
ที่อยู่ปัจจุบัน	บ้านเลขที่ 119/12 หมู่ที่ 2 ซอยเพิ่มสุข ถนนกาญจนาภิเษก ตำบลบางคูเวียง อำเภอบางกรวย จังหวัดนนทบุรี 11130
ประวัติการศึกษา	ปีการศึกษา 2561 สำเร็จการศึกษาหลักสูตรนิเทศศาสตรบัณฑิต (นศ.บ.) เกรดเฉลี่ย 3.97 (เกียรตินิยมอันดับหนึ่งเหรียญทอง) สาขาวิชาการประชาสัมพันธ์ มหาวิทยาลัยธุรกิจบัณฑิตย์
ประวัติการทำงาน	1 มิถุนายน 2562 - 30 พฤศจิกายน 2563 Public Relations Officer บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด (มหาชน) 1 ธันวาคม 2563 - ปัจจุบัน Solutions Specialist บริษัท ลานนาคอม จำกัด