

การหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่

ณัฐพล แสงเลิศศิลป์ชัย*

บริษัท หัวเว่ยเทคโนโลยี (ประเทศไทย) จำกัด

*Correspondence: pmuj21@gmail.com

doi: XXXXXX

บทคัดย่อ

งานวิจัยนี้มีวัตถุประสงค์ในการศึกษาถึงปัจจัยที่ส่งผลถึงการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ (Wearable Technology) ประกอบด้วยปัจจัย การรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม การรับรู้ถึงความรุนแรงของภัยคุกคาม การรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคาม การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคาม การรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ ความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัว ความกังวลในด้านความเป็นส่วนตัว และการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ โดยเก็บข้อมูลจากกลุ่มตัวอย่างจำนวน 173 คน

ผลการวิจัยพบว่าปัจจัยการรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม การรับรู้ถึงความรุนแรงของภัยคุกคาม และความกังวลในด้านความเป็นส่วนตัว ส่งผลทางตรงต่อการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ปัจจัยการรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคาม การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคาม และการรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม ส่งผลทางตรงต่อการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ปัจจัยการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ และการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ส่งผลทางตรงต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ โดยหากบุคคลเกิดความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ แล้วก็จะส่งผลโดยตรงไปยังการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ ด้วยเช่นกัน อย่างไรก็ตามผลการวิจัยยังพบว่า ปัจจัยความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวไม่ส่งอิทธิพลต่อความกังวลในด้านความเป็นส่วนตัว เนื่องจากผลการวิจัยไม่สนับสนุนสมมติฐานการวิจัย ซึ่งสาเหตุอาจมาจากการไม่สนใจและความไม่เข้าใจในตัวนโยบายคุ้มครองข้อมูลส่วนตัวจึงทำให้บุคคลไม่เกิดความกังวลในด้านความเป็นส่วนตัว

ผู้ให้บริการเทคโนโลยีสวมใส่สามารถนำผลที่ได้ไปปรับใช้เพื่อพัฒนาวิธีป้องกันภัยคุกคามโดยอาจเน้นไปที่การสร้างแรงจูงใจให้ผู้ใช้บริการเกิดความตั้งใจและทำการหลีกเลี่ยงภัยคุกคามที่เกิดขึ้น ในด้านของผู้ใช้บริการหรือบุคคลใกล้ชิดสามารถนำผลไปปรับใช้เพื่อสร้างแรงกระตุ้นให้บุคคลเกิดการหลีกเลี่ยงและหาทางป้องกันภัยคุกคามที่อาจเกิดขึ้นกับข้อมูลส่วนตัวได้

คำสำคัญ: การรับรู้ถึงภัยคุกคาม การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคาม ความตั้งใจในการหลีกเลี่ยงภัยคุกคาม การหลีกเลี่ยงภัยคุกคาม

Threat Avoidance Behavior of Privacy on Wearable Technology

Nattaphol Saenglertsilpachai*

Huawei Technologies (Thailand) Co. Ltd.

*Correspondence: pmuj21@gmail.com

doi: XXXXXX

Abstract

The purpose of this research is to study the factors influencing Behavior of Threat Avoidance on Wearable Technology which include factors Perceived Susceptibility, Perceived Severity, Perceived Threat, Perceived Effectiveness, Perceived Costs, Self-Efficacy, Perceived Avoidability, Avoidance Motivation, Revelation of Privacy Policy, Concern for Information Privacy and Avoidance Behavior. The data was collected from 173 participants who have experience in using Wearable Technology.

According to the results, this research found that Perceived Susceptibility, Perceived Severity and Concern for Information Privacy directly affect Perceived Threat. This research also found that Perceived Effectiveness, Perceived Costs and Self-Efficacy directly affect Perceived Avoidability. Moreover, this research found that Perceived Threat and Perceived Avoidability directly affect Avoidance Motivation. Also if participants are motivated to avoiding threat this motivation will directly affects their Avoidance Behavior as well. However, the results show that Revelation of Privacy Policy does not affect to Concern for Information Privacy. The reason could be that participants may not pay attention or do not understand the privacy policy well enough. So they did not concern even the privacy policy are relevant or not.

Wearable Technology provider can use these results to adapt and develop a safeguarding measure to motivate user to avoid threat. Also user and people around them can focus on how to convince each other to perceived benefit on threat avoidance and taking safeguarding measure to protect their personal information.

Keywords: Perceived Threat, Perceived Avoidability, Avoidance Motivation, Threat Avoidance Behavior

1. บทนำ

1.1 ความสำคัญและที่มาของปัญหาการวิจัย

ในปัจจุบันเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงที่รวดเร็วมาก มีเทคโนโลยีใหม่ ๆ เกิดขึ้นทุกวันและมีการพัฒนาอย่างต่อเนื่อง ผู้พัฒนาได้มองหาวิธีการใหม่ ๆ เพื่อให้ผู้ใช้งานสามารถเข้าถึงอินเทอร์เน็ตได้อย่างรวดเร็ว เทคโนโลยีสวมใส่ หรือ Wearable Technology จึงถูกพัฒนาเพื่อตอบสนองการเข้าถึงอินเทอร์เน็ตได้อย่างลงตัว (Hughes, 2014)

เทคโนโลยีสวมใส่ หมายถึง การนำเทคโนโลยีหรือคอมพิวเตอร์ไปฝังไว้ในอุปกรณ์ที่สามารถสวมใส่ได้ เช่น เสื้อผ้า แว่นตา หรือ นาฬิกา จึงทำให้อุปกรณ์เหล่านั้นสามารถเก็บข้อมูล รับส่งข้อมูลผ่านการสื่อสารไร้สาย และแสดงผลให้กับผู้ใช้งานตามเวลาจริงได้ (Hughes, 2014) ซึ่งข้อมูลต่าง ๆ ที่เก็บอยู่ในตัวเทคโนโลยีสวมใส่มีทั้งข้อมูลส่วนตัวของผู้ใช้ และข้อมูลที่ถูกบันทึกในชีวิตประจำวัน เช่น ข้อมูลสุขภาพ หรือข้อมูลการใช้จ่ายเงินสำหรับผู้ที่ต้องการวางแผนการใช้จ่าย ซึ่งข้อมูลเหล่านี้เมื่อถูกแสดงผลให้กับผู้ใช้งานตามเวลาจริงแล้วจะเป็นประโยชน์ทำให้ผู้ใช้งานสามารถเข้าใจตัวเองและพฤติกรรมของเขามากขึ้น (ภาวรุฑ พงษ์วิทย์ภานุ, 2557)

เทคโนโลยีสวมใส่สามารถสร้างประโยชน์ให้กับผู้ใช้งานได้มากมายมหาศาล เพราะเป็นอุปกรณ์ที่มีลักษณะพิเศษเฉพาะตัว คือมีการพกหรือสวมใส่ติดตัวตลอดเวลา เป็นเครื่องมือที่มีความเป็นส่วนตัวมากกว่าอุปกรณ์อื่น ๆ เช่น โน้ตบุ๊ก แท็บเล็ต หรือ โทรศัพท์มือถือสมาร์ทโฟน (Smart phone) อย่างไรก็ตามคุณลักษณะพิเศษเหล่านี้ก็นำมาซึ่งความเสี่ยงทางด้านความปลอดภัย ซึ่งความเสี่ยงต่าง ๆ ไม่ได้ทำอันตรายแค่กับข้อมูลของผู้ใช้งานเท่านั้น ยังสามารถก่อให้เกิดภัยอันตรายไปถึงตัวผู้ใช้งานเองได้อีกด้วย (Mills et al., 2016) ความเสี่ยงจากการที่มีการใช้เทคโนโลยีสวมใส่มากขึ้นทำให้เทคโนโลยีสวมใส่ตกเป็นเป้าหมายของอาชญากรในโลกไซเบอร์หรือแฮกเกอร์ที่เจาะเข้ามาสร้างความเสียหายโดยอาศัยช่องโหว่ของเทคโนโลยี เช่น การขโมยข้อมูลส่วนตัว หรือปัญหาการเรียกค่าไถ่ข้อมูลหรือที่เรียกว่า Ransomware ที่พุ่งเป้าหมายมาที่อุปกรณ์เทคโนโลยีสวมใส่ เช่น พวงนาฬิกาอัจฉริยะ (Smart Watch) และเครื่องติดตามความแอคทีฟ (Activity trackers) ที่มีเซ็นเซอร์มีโอกาสเสี่ยงสูงที่จะถูกเฝ้าติดตามข้อมูลส่วนตัวและกิจวัตรประจำวัน แฮกเกอร์สามารถขโมยข้อมูลส่วนตัวของผู้ใช้งานผ่านทาง อุปกรณ์เทคโนโลยีสวมใส่ได้ ดังนั้นเรื่องความปลอดภัยของเทคโนโลยีสวมใส่จึงควรเป็นสิ่งที่ทุกคนให้ความสำคัญ

1.2 วัตถุประสงค์ของการวิจัย

งานวิจัยนี้มีวัตถุประสงค์เพื่อศึกษาถึงปัจจัยต่าง ๆ ที่มีอิทธิพลต่อการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ ประกอบด้วย ความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัว ความกังวลในด้านความเป็นส่วนตัว การรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม การรับรู้ถึงความรุนแรงของภัยคุกคาม การรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคาม การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคาม การรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ที่ส่งผลต่อ การหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ผ่านความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

จากการศึกษางานวิจัยที่เกี่ยวข้องสามารถสรุปปัจจัยที่เกี่ยวข้องกับการศึกษาได้ดังนี้

การรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม (Perceived Susceptibility) หมายถึง การที่บุคคลรับรู้ถึงความเสี่ยงที่อาจเกิดขึ้นได้ของเทคโนโลยีสวมใส่ที่จะถูกโจมตีจากภัยคุกคามทางเทคโนโลยีสารสนเทศและทำอันตรายต่อข้อมูลส่วนตัวของพวกเขา (Claar, 2011; Liang & Xue, 2009)

การรับรู้ถึงความรุนแรงของภัยคุกคาม (Perceived Severity) หมายถึง การที่บุคคลรับรู้ถึงผลกระทบที่เกิดจากภัยคุกคามทางเทคโนโลยีสารสนเทศที่สามารถสร้างความเสียหายอย่างร้ายแรงต่อข้อมูลส่วนตัวและสร้างความเดือดร้อนให้กับตัวบุคคลเองได้ (Manzano, 2012; Liang & Xue, 2009)

การรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ (Perceived Threat) หมายถึง การรับรู้ถึงภัยอันตรายที่เกิดขึ้นจากการใช้เทคโนโลยีสวมใส่ที่เข้ามาทำอันตรายให้กับข้อมูลส่วนตัวของบุคคลได้ (Liang & Xue, 2010)

การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคาม (Perceived Effectiveness) หมายถึง การรับรู้ถึงผลลัพธ์จากการใช้มาตรการรักษาความปลอดภัยว่าจะสามารถป้องกันภัยจากความเสียหายที่อาจเกิดขึ้นได้ (Liang and Xue, 2009) และหากปฏิบัติตามมาตรการที่วางไว้จะนำไปสู่ผลลัพธ์ที่ต้องการและสามารถลดความเสี่ยงจากภัยคุกคามได้ (Bandura, 1982)

การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคาม (Perceived Costs) หมายถึง การที่บุคคลรับรู้ถึงต้นทุนที่เกิดจากการเลือกใช้มาตรการรักษาความปลอดภัย เช่น เวลา เงิน ความยุ่งยาก หรือการทำความเข้าใจในการใช้มาตรการรักษาความปลอดภัย รวมถึงการเปรียบเทียบค่าใช้จ่ายกับผลประโยชน์ที่ได้รับ (Weinstein, 1993; Liang & Xue, 2009)

การรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม (Self-Efficacy) หมายถึง การที่บุคคลเชื่อในความสามารถของตนเองในการควบคุมเหตุการณ์ต่าง ๆ ที่เกิดขึ้น (Rhee et al., 2009) โดยบุคคลจะมีความเชื่อว่าเขานั้นสามารถใช้มาตรการรักษาความปลอดภัยเพื่อที่จะหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ได้อย่างมีประสิทธิภาพ (Bandura, 1977)

การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ (Perceived Avoidability) หมายถึง การที่บุคคลรับรู้ว่ามาตรการรักษาความปลอดภัยจะสามารถช่วยในการป้องกันไม่ให้เกิดภัยคุกคามข้อมูลส่วนตัวได้มากน้อยเพียงใด (นิธิป ชวนตันติกมล, 2557)

ความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ (Avoidance Motivation) หมายถึง การที่บุคคลเคยได้รับภัยคุกคามที่อาจเข้ามาทำอันตรายต่อข้อมูลส่วนตัว ทำให้เกิดแรงกระตุ้นในการหลีกเลี่ยงภัยคุกคามเหล่านั้น (นิธิป ชวนตันติกมล, 2557) โดยผู้ใช้งานจะถูกแรงกระตุ้นให้เกิดการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการเลือกใช้มาตรการรักษาความปลอดภัย (Liang & Xue, 2009)

ความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัว (Revelation of Privacy Policy) หมายถึง การเปิดเผยถึงรายละเอียดต่าง ๆ ที่ผู้ให้บริการปฏิบัติต่อข้อมูลส่วนตัวของผู้ใช้บริการในเรื่องของการเก็บข้อมูลส่วนตัวและการนำข้อมูลส่วนตัวไปใช้ ซึ่งจะถูกเขียนรวมไว้ ณ ที่ใดที่หนึ่งเพื่อให้ผู้ให้บริการสามารถเข้าไปอ่านได้ (Kuo et al., 2015)

ความกังวลในด้านความเป็นส่วนตัว (Concern for Information Privacy) หมายถึง การที่บุคคลให้ความสำคัญอย่างมากเกี่ยวกับการเก็บข้อมูลส่วนตัวและการถูกนำข้อมูลส่วนตัวไปใช้ (Son & Kim, 2008) โดยบุคลิกลักษณะของบุคคลที่มีแนวโน้มที่จะกังวลเกี่ยวกับเรื่องข้อมูลส่วนตัวนั้น จะรู้สึกไม่สบายใจและกลัวว่าผู้อื่นจะนำข้อมูลส่วนตัวของเขาไปใช้ในทางที่ไม่เหมาะสม (Edwards, 2015)

การหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ (Avoidance Behavior) หมายถึง การดำเนินการเพื่อให้ตัวเองหลุดพ้นจากภัยอันตรายและความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ (Liang & Xue, 2009)

H2: การรับรู้ถึงความรุนแรงของภัยคุกคามส่งผลเชิงบวกถึงการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่

ผู้ใช้งานเทคโนโลยีจะรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามเมื่อรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคามหรือมาตรการรักษาความปลอดภัยว่าจะสามารถลดความเสี่ยงในการเกิดภัยคุกคามได้อย่างมีประสิทธิภาพ (Liang & Xue, 2009) ผู้ใช้งานจะประเมินถึงมาตรการรักษาความปลอดภัยโดยเทียบกับผลลัพธ์ หากปฏิบัติตามมาตรการรักษาความปลอดภัยนั้นแล้วสามารถได้ผลลัพธ์ตามที่ต้องการคือสามารถลดความเสี่ยงหรือหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวได้ ผู้ใช้งานจะรับรู้ถึงภัยคุกคามนั้นสามารถที่จะหลีกเลี่ยงได้ (Bandura, 1982) ซึ่งผู้ใช้งานมีโอกาสมากขึ้นที่จะรับรู้ถึงภัยคุกคามนั้นสามารถหลีกเลี่ยงได้เมื่อวิธีป้องกันภัยหรือมาตรการรักษาความปลอดภัยนั้นสามารถป้องกันภัยได้อย่างมีประสิทธิภาพ จึงนำไปสู่ข้อสมมติฐานได้ดังนี้

H3: การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคามส่งผลเชิงบวกถึงการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่

การที่ผู้ใช้งานเทคโนโลยีจะรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามนอกเหนือจากการที่เขารับรู้ถึงประสิทธิภาพของมาตรการรักษาความปลอดภัยแล้วยังต้องคำนึงถึงค่าใช้จ่ายของมาตรการรักษาความปลอดภัยนั้นอีกด้วย ซึ่งการรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคามถือเป็นอุปสรรคสำคัญในการเลือกใช้มาตรการรักษาความปลอดภัย (Ng et al., 2009) ผู้ใช้งานมีโอกาสมากขึ้นที่จะรับรู้ถึงภัยคุกคามนั้นสามารถหลีกเลี่ยงได้เมื่อเขารับรู้ถึงค่าใช้จ่ายนั้นลดลงต่ำกว่าประโยชน์ที่เขาได้รับ ซึ่งถ้าหากค่าใช้จ่ายที่เขาได้รับมีมากกว่าประโยชน์ที่เขาได้รับเขาก็มีแนวโน้มที่จะไม่เลือกใช้มาตรการรักษาความปลอดภัยนั้น (Liang & Xue, 2009) จึงนำไปสู่ข้อสมมติฐานได้ดังนี้

H4: การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคามส่งผลเชิงลบถึงการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่

การที่บุคคลรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม คือการที่เขามีความเชื่อว่าตัวเองจะสามารถปฏิบัติตามมาตรการที่ต้องการเพื่อที่จะหลีกเลี่ยงภัยคุกคามได้ (Maddux & Rogers, 1983) ซึ่งการรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคามของผู้ใช้งานจะส่งผลกระทบอย่างมากถึงมุมมองที่ผู้ใช้งานมีต่อประโยชน์ของมาตรการรักษาความปลอดภัย บุคคลอาจคิดว่ามาตรการรักษาความปลอดภัยที่เขาปฏิบัติไม่สมารถที่จะช่วยให้เขาหลีกเลี่ยงภัยคุกคามได้เพราะว่าเขาไม่มั่นใจและคิดว่าตัวเองไม่มีความสามารถพอในการใช้มาตรการเหล่านั้น แม้ว่ามาตรการจะมีประสิทธิภาพและมีราคาถูกลงก็ตาม (Liang & Xue, 2009) ดังนั้นผู้ที่มั่นใจในตนเองว่าเขาสามารถใช้มาตรการรักษาความปลอดภัยได้อย่างมีประสิทธิภาพมีโอกาสมากขึ้นที่จะรับรู้ถึงภัยคุกคามนั้นสามารถหลีกเลี่ยงได้ จึงนำไปสู่ข้อสมมติฐานได้ดังนี้

H5: การรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคามส่งผลเชิงบวกถึงการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่

เมื่อผู้ใช้งานพบว่าเขาถูกภัยคุกคามพวกเขาจะถูกกระตุ้นให้เกิดการป้องกันตัวเองซึ่งเป็นธรรมชาติของมนุษย์ (Liang & Xue, 2009) จากงานวิจัยทางด้านจิตวิทยาสุขภาพแสดงให้เห็นว่าปัญหาสุขภาพทำให้เกิดการรับรู้ถึงภัยคุกคามและนำไปสู่ความตั้งใจในการปกป้องตัวเองจากภัยคุกคามเหล่านั้น (Janz & Becker, 1984; Oliver & Berger, 1979; Rosenstock, 1974) การรับรู้ถึงภัยคุกคามของโรคต่าง ๆ ทำให้บุคคลเกิดความตั้งใจในการดูแลสุขภาพมากขึ้น

จากงานวิจัยของ Claar (2011) และ Ng et al. (2009) พบว่าการรับรู้ถึงภัยคุกคามกระตุ้นให้เกิดพฤติกรรมการรักษาความปลอดภัยได้ การรับรู้ถึงภัยคุกคามจึงเป็นตัวกำหนดถึงแรงจูงใจและความตั้งใจในการกระทำการรักษาความปลอดภัยและหลีกเลี่ยงจากภัยคุกคาม จึงนำไปสู่ข้อสมมติฐานได้ดังนี้

H6: การรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ส่งผลเชิงบวกถึงความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่

จากทฤษฎีความคาดหวัง (Steers et al., 2004) ผู้ใช้งานจะถูกกระตุ้นให้เลือกมาตรการรักษาความปลอดภัยที่ให้ผลลัพธ์ที่ดีที่สุด ดังนั้นผู้ใช้งานจะถูกจูงใจให้เลือกใช้มาตรการรักษาความปลอดภัยที่สามารถหลีกเลี่ยงภัยคุกคามได้มากที่สุด การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามสะท้อนถึงความสามารถในการควบคุมการใช้มาตรการรักษาความปลอดภัยของผู้ใช้งานที่จะรับมือกับภัยคุกคามที่เกิดขึ้น เมื่อผู้ใช้งานรับรู้ว่าตนเองมีความสามารถที่จะหลีกเลี่ยงภัยคุกคามได้ ก็จะทำให้เกิดความตั้งใจที่จะใช้มาตรการรักษาความปลอดภัยที่สามารถป้องกันภัยคุกคามเหล่านั้นได้ (Liang & Xue, 2009) จึงนำไปสู่ข้อสมมติฐานได้ดังนี้

H7: การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ส่งผลเชิงบวกถึงความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่

มนุษย์มักจะถูกกระตุ้นให้เกิดการกระทำซ้ำๆ จากผลลัพธ์ที่น่าพอใจในอดีต และถูกกระตุ้นให้ลดการกระทำที่ส่งผลไม่ดีในอดีตลง บุคคลจะเลือกแสดงพฤติกรรมที่คิดว่าเมื่อเลือกไปแล้วจะเกิดผลลัพธ์ที่มีคุณค่า จากทฤษฎีความคาดหวัง Steers et al. (2004) ได้กล่าวไว้ว่าบุคคลมีแนวโน้มที่จะแสดงพฤติกรรมเมื่อเขาเกิดแรงจูงใจและความตั้งใจต่อพฤติกรรมนั้น ดังนั้นในแง่ของเทคโนโลยีบุคคลที่มีความตั้งใจในการหลีกเลี่ยงภัยคุกคามมีแนวโน้มที่จะเลือกใช้มาตรการรักษาความปลอดภัยที่สามารถทำให้เขาลดหรือหลีกเลี่ยงภัยคุกคามได้ (Liang & Xue, 2009) จึงนำไปสู่ข้อสมมติฐานได้ดังนี้

H8: ความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ส่งผลเชิงบวกถึงการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่

ในการคุ้มครองข้อมูลส่วนตัวของผู้ใช้บริการ ผู้ให้บริการสามารถสร้างความน่าเชื่อถือโดยการออกนโยบายคุ้มครองข้อมูลส่วนตัว ซึ่งผู้ให้บริการจะรู้สึกสบายใจและมั่นใจที่จะใช้บริการเมื่อมีการระบุนโยบายคุ้มครองข้อมูลส่วนตัวอย่างชัดเจน และสามารถบอกเป็นนัยได้ว่าผู้ให้บริการจะมีความกังวลในข้อมูลส่วนตัวลดลงเมื่อผู้ให้บริการออกนโยบายคุ้มครองข้อมูลส่วนตัวอย่างเปิดเผย ดังนั้น การมีนโยบายคุ้มครองข้อมูลส่วนตัวจึงทำให้ผู้ให้บริการลดความกังวลในด้านความเป็นส่วนตัวลงไปได้ นำไปสู่ข้อสมมติฐานได้ดังนี้

H9: ความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวส่งผลเชิงลบถึงความกังวลในด้านความเป็นส่วนตัว

ความกังวลในด้านความเป็นส่วนตัวคือลักษณะส่วนบุคคลของคนที่มีความวิตกกังวลในเรื่องข้อมูลส่วนตัว Van et al. (2006) พบว่าความกังวลในด้านความเป็นส่วนตัวส่งผลถึงการรับรู้ความเสี่ยงและความไม่ไว้วางใจของลูกค้าในการซื้อของออนไลน์ คนที่มีความกังวลในด้านความเป็นส่วนตัวมักจะมีแนวโน้มเชื่อว่าบริษัทที่ให้บริการออนไลน์นั้นจะสามารถนำข้อมูลส่วนตัวของพวกเขาไปใช้ได้ทำให้เขารับรู้ถึงความเสี่ยงและรับรู้ถึงภัยคุกคามที่อาจเกิดขึ้น (Dinev &

Hart, 2006; Van et al., 2006) ดังนั้นความกังวลในด้านความเป็นส่วนตัวของผู้ใช้งานเทคโนโลยีจึงส่งผลถึงการรับรู้ภัยคุกคามในด้านความปลอดภัยนำไปสู่ข้อสมมติฐานได้ดังนี้

H10: ความกังวลในด้านความเป็นส่วนตัวส่งผลเชิงบวกถึงการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่

4. วิธีการวิจัย

งานวิจัยนี้เป็นงานวิจัยเชิงปริมาณ (Quantitative Research) เครื่องมือที่ใช้ในการวิจัยครั้งนี้คือ แบบสอบถาม (Questionnaire) ซึ่งพัฒนามาจากงานวิจัยในอดีต โดยก่อนการจัดเก็บข้อมูลจากกลุ่มตัวอย่างได้นำแบบสอบถามไปทดสอบกับกลุ่มตัวอย่างจำนวน 48 คน เพื่อวิเคราะห์ความเหมาะสมของแบบสอบถามและปรับปรุงข้อคำถามให้มีความเหมาะสมเพื่อนำไปจัดเก็บข้อมูลจริง หลังจากนั้นได้ทำการเก็บข้อมูลจริงโดยการแจกแบบสอบถามอิเล็กทรอนิกส์ผ่านทางสื่อสังคมออนไลน์ ได้แก่ เฟซบุ๊ก (Facebook) โดยกระจายไปยังหน้าเพจของกลุ่มต่างๆ ในเฟซบุ๊ก อาทิ เช่น กลุ่ม Apple Watch User Thailand, Fitbit Users Thailand, Samsung Gear S3 Thailand, Apple Watch Fitness Thailand, SmartWatch Club Thailand (annth), Garmin Club แลกเปลี่ยนความรู้ เทคนิค โดย BananaRun, และ MSMIS CLUB โดยเริ่มส่งในช่วงเดือนมิถุนายน 2560 และแจกแบบสอบถามแบบกระดาษผ่านคนรู้จักทั้งในองค์กรและนอกองค์กรที่เคยใช้อุปกรณ์เทคโนโลยีสวมใส่ โดยมีผู้ตอบแบบสอบถามที่เคยใช้อุปกรณ์เทคโนโลยีสวมใส่ทั้งหมด 180 คน โดยมาจากแบบสอบถามอิเล็กทรอนิกส์ 155 คน และแบบสอบถามแบบกระดาษ 25 คน

5. ผลการวิจัย

5.1 การทดสอบข้อตกลงเบื้องต้นทางสถิติ

ข้อมูลที่จัดเก็บจากกลุ่มตัวอย่างถูกนำไปทดสอบข้อตกลงเบื้องต้นทางสถิติ ผ่านการทดสอบหาข้อมูลขาดหาย (Missing Data) การทดสอบหาข้อมูลสุดโต่ง (Outliers) และการทดสอบการกระจายของข้อมูล (Frequencies) ซึ่งจากการทดสอบพบว่าข้อมูลไม่มีส่วนใดขาดหาย ส่วนการทดสอบหาข้อมูลสุดโต่งพบว่ามี 7 ตัวอย่างที่ตอบแบบสอบถามแบบสุดโต่ง ซึ่งส่งผลต่อค่าสถิติอื่นๆ จึงพิจารณาตัดตัวอย่างดังกล่าวออก และจากการทดสอบข้อมูลดังกล่าวพบว่ามีข้อมูลบางปัจจัยที่ไม่มีการกระจายแบบปกติ กล่าวคือมีการกระจายข้อมูลแบบเบ้ซ้าย แต่มีความเบ้ไม่ต่างจากเกณฑ์มาตรฐานมากนักจึงยังคงใช้ข้อมูลดังกล่าวเพื่อวิเคราะห์ข้อมูลทางสถิติในขั้นตอนต่อไป

5.2 การประเมินความเที่ยงและความตรงของแบบสอบถาม

งานวิจัยนี้ได้ตรวจสอบความเที่ยงของแบบสอบถาม (Reliability) ด้วยการวิเคราะห์ค่าสัมประสิทธิ์แอลฟาของครอนบราซ (Cronbach's Alpha) โดยใช้เกณฑ์ที่มีค่ามากกว่า 0.7 ขึ้นไป ซึ่งถือว่าเป็นระดับที่มีความเชื่อถือได้ในงานวิจัยแบบ Basic Research (Hair et al., 1998) นอกจากนี้ยังได้ตรวจสอบความตรงของแบบสอบถาม (Validity) ด้วยการวิเคราะห์องค์ประกอบ (Factor Analysis) จากการหมุนแกนในลักษณะของ Varimax rotation โดยต้องมีค่าน้ำหนักองค์ประกอบ (Factor Loading) ไม่ต่ำกว่า 0.5 ซึ่งการทดสอบในแต่ละตัวแปรถือว่าผ่านเกณฑ์ทั้งหมด โดยมีรายละเอียด ดังตารางที่ 1

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน น้ำหนักองค์ประกอบ และค่าสัมประสิทธิ์แอลฟาของครอนบราซ
ของตัวแปรทั้งหมด

ตัวแปร	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 1: การรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม (% of variance = 66.511, Cronbach's alpha = 0.832)			
ท่านคิดว่ามีความเป็นไปได้ที่เทคโนโลยีสวมใส่ที่ท่านสวมใส่อยู่จะมีช่องโหว่ทำให้ถูกคุกคามจากไวรัสหรือสปายแวร์ได้	3.618	0.9966	0.870
ท่านคิดว่าเทคโนโลยีสวมใส่ที่ท่านสวมใส่อยู่นั้นสามารถถูกเจาะเข้าระบบโดยแฮกเกอร์ได้	3.520	0.9559	0.821
ท่านคิดว่ามีความเป็นไปได้ที่ข้อมูลส่วนตัวของท่านอาจจะถูกขโมยจากการสวมใส่เทคโนโลยีสวมใส่	3.601	0.9868	0.805
ท่านคิดว่าในอนาคตอุปกรณ์เทคโนโลยีสวมใส่ของท่านมีแนวโน้มที่จะติดไวรัสหรือสปายแวร์ได้	3.636	0.8959	0.761
ปัจจัยที่ 2: การรับรู้ถึงความรุนแรงของภัยคุกคาม (% of variance = 62.949, Cronbach's alpha = 0.800)			
ท่านคิดว่าไวรัสและสปายแวร์สามารถบุกรุกความเป็นส่วนตัวส่วนตัวของท่านได้	3.775	1.1160	0.875
ท่านคิดว่าไวรัสและสปายแวร์สามารถขโมยข้อมูลส่วนตัวของท่านโดยที่ท่านไม่รู้ตัวได้	4.012	0.9644	0.846
ท่านคิดว่าการที่อุปกรณ์เทคโนโลยีสวมใส่ของท่านติดไวรัสหรือสปายแวร์ทำให้แฮกเกอร์สามารถนำข้อมูลส่วนตัวของท่านไปใช้เพื่อก่ออาชญากรรมทางอินเทอร์เน็ตได้	3.746	1.0477	0.763
ท่านคิดว่าการที่อุปกรณ์เทคโนโลยีสวมใส่ของท่านติดไวรัสหรือสปายแวร์ทำให้ระบบในอุปกรณ์ของท่านเกิดความเสียหายไม่สามารถใช้งานได้	3.682	0.9986	0.674
ปัจจัยที่ 3: การรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ (% of variance = 65.856, Cronbach's alpha = 0.821)			
ท่านคิดว่าการที่แฮกเกอร์พยายามเข้าถึงข้อมูลส่วนตัวของท่านผ่านอุปกรณ์เทคโนโลยีสวมใส่เป็นสิ่งที่เป็นอันตรายต่อข้อมูลส่วนตัวของท่าน	3.936	0.9223	0.882
ท่านคิดว่าเป็นเรื่องที่น่ากลัวหากข้อมูลสำคัญของท่านถูกขโมยไปจากอุปกรณ์เทคโนโลยีสวมใส่ของท่าน	3.971	1.0367	0.871
ท่านคิดว่ามีความเสี่ยงที่ข้อมูลส่วนตัวของท่านจะถูกนำไปใช้โดยไม่ได้ยินยอมหากท่านใช้เทคโนโลยีสวมใส่ที่ติดไวรัสหรือสปายแวร์	3.890	0.9732	0.801
ไวรัสและสปายแวร์เป็นสิ่งที่เป็นอันตรายต่อข้อมูลส่วนตัวของท่าน	4.058	1.0213	0.674

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน หน้าหน้าองค์ประกอบ และค่าสัมประสิทธิ์แอลฟาของครอนบราซของตัวแปรทั้งหมด (ต่อ)

ตัวแปร	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 4: การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคาม (% of variance = 61.012, Cronbach's alpha = 0.839)			
ท่านรู้สึกมั่นใจว่าเมื่อใช้แอปพลิเคชันป้องกันแล้วจะสามารถปกป้องข้อมูลส่วนตัวของท่านได้	3.376	0.9294	0.826
ท่านรู้สึกมั่นใจว่าเมื่อท่านตั้งค่าความเป็นส่วนตัว (Privacy Setting) ผ่านแอปพลิเคชันที่เชื่อมต่อกับอุปกรณ์เทคโนโลยีสวมใส่แล้วจะสามารถปกป้องข้อมูลส่วนตัวของท่านได้	3.474	0.9122	0.825
ท่านคิดว่าการตั้งค่าความเป็นส่วนตัว (Privacy Setting) ผ่านแอปพลิเคชันที่เชื่อมต่อกับอุปกรณ์เทคโนโลยีสวมใส่สามารถปกป้องข้อมูลส่วนตัวของท่านได้	3.543	0.9242	0.798
ท่านคิดว่าแอปพลิเคชันป้องกันเช่น Activation Lock สามารถช่วยป้องกันไม่ให้ข้อมูลส่วนตัวของท่านถูกขโมยได้	3.410	0.9396	0.762
ท่านคิดว่าการเปลี่ยนรหัสผ่านของอุปกรณ์ที่เชื่อมต่อกับเทคโนโลยีสวมใส่อยู่เสมอสามารถช่วยปกป้องข้อมูลส่วนตัวของท่านได้	3.746	0.9176	0.686
ปัจจัยที่ 5: การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคาม (% of variance = 63.838, Cronbach's alpha = 0.710)			
ท่านจะไม่ใช้แอปพลิเคชันเพื่อป้องกันภัยคุกคามถ้าแอปพลิเคชันนั้นมีค่าใช้จ่ายมากกว่าประโยชน์ที่ได้รับ	3.676	1.2053	0.897
ท่านจะเปรียบเทียบผลประโยชน์และค่าใช้จ่ายก่อนที่จะตัดสินใจใช้แอปพลิเคชันเพื่อป้องกันภัยคุกคาม	3.983	1.0085	0.763
ท่านจะไม่ตั้งค่าความเป็นส่วนตัว (Privacy Setting) ผ่านแอปพลิเคชันที่เชื่อมต่อกับอุปกรณ์เทคโนโลยีสวมใส่ ถ้าหากการตั้งค่านั้นมีความยุ่งยากมากกว่าประโยชน์ที่ได้รับ	3.272	1.2488	0.727
ปัจจัยที่ 6: การรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม (% of variance = 72.341, Cronbach's alpha = 0.807)			
ท่านมั่นใจว่าสามารถตรวจจับไม่ให้ไวรัสหรือสปายแวร์ผ่านเข้ามาในอุปกรณ์เทคโนโลยีสวมใส่ของท่านได้	3.532	0.9737	0.914
ท่านมั่นใจว่าสามารถจัดการกับไวรัสหรือสปายแวร์ผ่านการตั้งค่าความเป็นส่วนตัว (Privacy Setting) ในแอปพลิเคชันที่เชื่อมต่อกับอุปกรณ์เทคโนโลยีสวมใส่ของท่านได้	3.509	1.0434	0.883
การตั้งค่าความเป็นส่วนตัว (Privacy Setting) ผ่านแอปพลิเคชันที่เชื่อมต่อกับอุปกรณ์เทคโนโลยีสวมใส่เป็นเรื่องที่ท่านสามารถทำได้	4.052	0.8089	0.745

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน หน้าหน้าองค์ประกอบ และค่าสัมประสิทธิ์แอลฟาของครอนบราซของตัวแปรทั้งหมด (ต่อ)

ตัวแปร	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 7: การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ (% of variance = 78.166, Cronbach's alpha = 0.859)			
ท่านจะศึกษานโยบายการรักษาความเป็นส่วนตัวของอุปกรณ์เทคโนโลยีสวมใส่อย่างระมัดระวังก่อนเริ่มต้นใช้งานเทคโนโลยีสวมใส่	3.410	0.9938	0.922
ท่านจะติดตามข่าวสารความเคลื่อนไหวของเทคโนโลยีสวมใส่ในด้านการรักษาความปลอดภัยของข้อมูลอยู่เสมอ	3.364	1.0567	0.872
ท่านจะศึกษาการตั้งค่าความเป็นส่วนตัว (Privacy Setting) ก่อนเริ่มต้นใช้งานเทคโนโลยีสวมใส่	3.728	0.9283	0.858
ปัจจัยที่ 8: ความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ (% of variance = 71.172, Cronbach's alpha = 0.788)			
ท่านวางแผนที่จะใช้แอปพลิเคชันป้องกันเช่น Activation Lock เพื่อช่วยท่านหลีกเลี่ยงการคุกคามจากแฮกเกอร์ในอนาคต	3.566	0.8908	0.922
ท่านตั้งใจที่จะใช้แอปพลิเคชันป้องกันเช่น Activation Lock เพื่อช่วยท่านหลีกเลี่ยงการคุกคามจากแฮกเกอร์	3.595	0.9452	0.883
ท่านคาดว่า การตั้งค่าความเป็นส่วนตัว (Privacy Setting) สามารถช่วยท่านหลีกเลี่ยงการคุกคามจากแฮกเกอร์ได้	3.636	0.9647	0.710
ปัจจัยที่ 9: ความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัว (% of variance = 73.606, Cronbach's alpha = 0.818)			
นโยบายของแอปพลิเคชันที่เชื่อมต่อกับอุปกรณ์เทคโนโลยีสวมใส่ของท่านควรที่จะอธิบายถึงรายละเอียดในการนำข้อมูลส่วนตัวของท่านไปใช้	4.046	0.8681	0.883
นโยบายของแอปพลิเคชันที่เชื่อมต่อกับอุปกรณ์เทคโนโลยีสวมใส่ของท่านควรที่จะอธิบายถึงเหตุผลในการเก็บข้อมูลส่วนตัว	3.988	0.8352	0.859
นโยบายของแอปพลิเคชันที่เชื่อมต่อกับอุปกรณ์เทคโนโลยีสวมใส่ของท่านควรที่จะเปิดเผยว่าข้อมูลส่วนตัวอะไรบ้างที่ถูกจัดเก็บ	3.960	0.9484	0.831
ปัจจัยที่ 10: ความกังวลในด้านความเป็นส่วนตัว (% of variance = 78.380, Cronbach's alpha = 0.862)			
ท่านรู้สึกไม่สบายใจว่าคนอื่นจะสามารถพบเจอข้อมูลส่วนตัวของท่านที่อยู่ในอุปกรณ์เทคโนโลยีสวมใส่ของท่าน	3.821	1.0439	0.905
ท่านรู้สึกไม่สบายใจว่าข้อมูลส่วนตัวของท่านที่อยู่ในอุปกรณ์เทคโนโลยีสวมใส่จะถูกนำไปใช้ในทางที่ผิด	3.850	1.0623	0.890
ท่านรู้สึกไม่สบายใจที่จะใส่ข้อมูลส่วนตัวที่สำคัญของท่านลงไปให้อุปกรณ์เทคโนโลยีสวมใส่ของท่าน	3.665	1.0526	0.860

ตารางที่ 1 ค่าเฉลี่ย ค่าเบี่ยงเบนมาตรฐาน หน้าหน้าองค์ประกอบ และค่าสัมประสิทธิ์แอลฟาของครอนบราซของตัวแปรทั้งหมด (ต่อ)

ตัวแปร	ค่าเฉลี่ย	ค่าเบี่ยงเบนมาตรฐาน	น้ำหนักองค์ประกอบ
ปัจจัยที่ 11: การหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ (% of variance = 56.568, Cronbach's alpha = 0.741)			
ท่านจะทำการเปลี่ยนรหัสผ่านของท่านอย่างสม่ำเสมอเพื่อป้องกันภัยคุกคาม	3.595	1.0611	0.786
ท่านจะเลือกใช้แอปพลิเคชันป้องกันเช่น Activation lock เพื่อป้องกันการคุกคามจากแฮกเกอร์	3.665	1.0246	0.781
ท่านจะทำการตั้งค่าความเป็นส่วนตัว (Privacy Setting) เพื่อหลีกเลี่ยงการคุกคามจากแฮกเกอร์	4.104	0.8563	0.752
ท่านจะทำการอัปเดตซอฟต์แวร์ในอุปกรณ์เทคโนโลยีสวมใส่ให้เป็นเวอร์ชันล่าสุดอยู่เสมอเพื่อหลีกเลี่ยงภัยคุกคาม	4.295	0.7699	0.685

5.3 ลักษณะทางประชากรศาสตร์ของกลุ่มตัวอย่าง

กลุ่มตัวอย่างส่วนใหญ่เป็นเพศหญิง (ร้อยละ 56.1) อายุของกลุ่มตัวอย่างส่วนใหญ่อยู่ระหว่าง 30-35 ปี (ร้อยละ 39.9) ระดับการศึกษาส่วนใหญ่อยู่ในระดับปริญญาตรี (ร้อยละ 53.8) มีอาชีพเป็นพนักงานบริษัทเอกชนมากที่สุด (ร้อยละ 68.2) โดยมีรายได้ต่อเดือนอยู่ในช่วงมากกว่า 50,000 บาทมากที่สุด (ร้อยละ 35.2) และใช้อุปกรณ์เทคโนโลยีสวมใส่ประเภทนาฬิกาข้อมือ (Smart watch) มากที่สุด (ร้อยละ 61.2)

5.4 การทดสอบสมมติฐานการวิจัย

งานวิจัยนี้ใช้การวิเคราะห์การถดถอยแบบเชิงชั้น (Hierarchical regression) ซึ่งวิเคราะห์หาอิทธิพลทางตรงและทางอ้อมของปัจจัยในกรอบแนวคิดการวิจัย โดยสามารถวิเคราะห์ผลได้ดังนี้

5.4.1 ผลการวิเคราะห์ตัวแปรอิสระที่ส่งผลถึงความกังวลในด้านความเป็นส่วนตัว

จากผลทางสถิติแสดงให้เห็นว่า ความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวส่งอิทธิพลทางตรงต่อความกังวลในด้านความเป็นส่วนตัว ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.261 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.001 และมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 6.8 ($R^2 = 0.068$) จากการวิเคราะห์พบว่าความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวไม่สอดคล้องกับสมมติฐานการวิจัยที่ 9 ที่กล่าวว่าความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวส่งผลเชิงลบถึงความกังวลในด้านความเป็นส่วนตัว เนื่องจากค่าสัมประสิทธิ์อิทธิพลมีค่าเป็นบวกทำให้ความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวส่งผลในทิศทางตรงกันข้ามกับสมมติฐานที่ตั้งไว้ โดยอาจมีสาเหตุมาจากการที่ผู้ใช้งานส่วนใหญ่ไม่สนใจหรืออาจไม่เข้าใจในนโยบายคุ้มครองข้อมูลส่วนตัวของผู้ให้บริการ จากการสำรวจผู้ใช้งานอินเทอร์เน็ตในสังคมออนไลน์พบว่า ผู้ใช้งานอินเทอร์เน็ตที่อ่านนโยบายคุ้มครองข้อมูลส่วนตัวมีเพียงร้อยละ 16 และจากสถิติผู้ที่อ่านพบว่ามีเพียงร้อยละ 20 ที่เข้าใจในตัวนโยบายคุ้มครองข้อมูลส่วนตัว (Dachis, 2012) ดังนั้น ถึงแม้จะมีการเปิดเผยนโยบายคุ้มครองข้อมูลส่วนตัวอย่างโปร่งใสก็อาจไม่ส่งผลให้ความกังวลในด้านความเป็นส่วนตัวนั้นลดลงเนื่องมาจากการไม่สนใจและความไม่เข้าใจในนโยบาย จึงทำให้ผลข้อมูลที่ได้ไม่สอดคล้องกับสมมติฐาน

5.4.2 ผลการวิเคราะห์ตัวแปรอิสระที่ส่งผลถึงการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่

จากผลทางสถิติแสดงให้เห็นว่า การรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม การรับรู้ถึงความรุนแรงของภัยคุกคาม ความกังวลในด้านความเป็นส่วนตัว และความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัว ส่งอิทธิพลต่อการรับรู้ถึงภัยคุกคาม

ข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 47.1 ($R^2 = 0.471$) ซึ่งมีรายละเอียดในแต่ละปัจจัยดังนี้

5.4.2.1 การรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม ส่งอิทธิพลทางตรงต่อการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.140 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.020 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 1 ที่กล่าวว่า การรับรู้ถึงโอกาสที่จะเกิดภัยคุกคามส่งผลเชิงบวกถึงการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) และ Claar (2011) ที่กล่าวว่า บุคคลที่รับรู้โอกาสที่จะเกิดภัยคุกคามได้มากจะรับรู้ถึงภัยคุกคามได้มากกว่าคนที่ไม่ได้รับรู้ถึงโอกาสที่จะเกิดภัยคุกคามหรือรับรู้ได้น้อยกว่า ดังนั้นเมื่อบุคคลรับรู้ถึงโอกาสเสี่ยงที่จะเกิดภัยคุกคามก็จะทำให้เขารับรู้ถึงภัยคุกคามนั้นตามไปด้วย

5.4.2.2 การรับรู้ถึงความรุนแรงของภัยคุกคาม ส่งอิทธิพลทางตรงต่อการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.481 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.000 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 2 ที่กล่าวว่า การรับรู้ถึงความรุนแรงของภัยคุกคามส่งผลเชิงบวกถึงการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ซึ่งสอดคล้องกับงานวิจัยของ Glanz et al. (2008) และ Liang and Xue (2009) ที่กล่าวว่า ความรุนแรงของภัยคุกคามจะส่งผลถึงการรับรู้ถึงภัยคุกคาม ถ้าหากภัยคุกคามที่เกิดขึ้นมีความรุนแรงและอันตรายถึงชีวิตจะทำให้การรับรู้ถึงภัยคุกคามมีมากตามความรุนแรงที่รับรู้ได้

5.4.2.3 ความกังวลในด้านความเป็นส่วนตัว ส่งอิทธิพลทางตรงต่อการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.284 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.000 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 10 ที่กล่าวว่า ความกังวลในด้านความเป็นส่วนตัวส่งผลเชิงบวกถึงการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ซึ่งสอดคล้องกับงานวิจัยของ Sim (2010), Dinev and Hart (2006) และ Edwards (2015) ที่กล่าวว่า ความกังวลในด้านความเป็นส่วนตัวส่งผลถึงการรับรู้ถึงภัยคุกคาม ดังนั้น ผู้ที่มีความกังวลด้านความเป็นส่วนตัวสูงมีแนวโน้มที่จะเห็นถึงผลในทางลบจากการเปิดเผยข้อมูลส่วนตัวได้มากทำให้เขาเกิดการรับรู้ถึงภัยคุกคามในข้อมูลส่วนตัวได้มากเช่นกัน

5.4.2.4 ความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัว ส่งอิทธิพลทางอ้อมต่อการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.074 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05 โดยค่าสัมประสิทธิ์มีค่าเป็นบวกทำให้ส่งผลตรงข้ามกับสมมติฐานที่ตั้งไว้ ซึ่งอาจมีสาเหตุตามที่ได้กล่าวไปในข้อ 5.4.1

5.4.3 ผลการวิเคราะห์ตัวแปรอิสระที่ส่งผลถึงการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่

จากผลทางสถิติแสดงให้เห็นว่า การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคาม การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคาม และการรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม ส่งอิทธิพลต่อการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 17.8 ($R^2 = 0.178$) ซึ่งมีรายละเอียดในแต่ละปัจจัยดังนี้

5.4.3.1 การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคาม ส่งอิทธิพลทางตรงต่อความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.217 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.004 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 3 ที่กล่าวว่า การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคามส่งผลเชิงบวกถึงการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ซึ่งสอดคล้องกับงานวิจัยของ Bandura (1982) และ Liang and Xue (2009) ที่กล่าวว่า ผู้ใช้งานเทคโนโลยีจะรับรู้ถึงภัยคุกคามเทคโนโลยีสามารถหลีกเลี่ยงได้ก็ต่อเมื่อเขารับรู้ว่ามาตรการรักษาความปลอดภัยที่เขาใช้นั้นมีประสิทธิภาพ ดังนั้น เมื่อผู้ใช้งานรับรู้ถึงประสิทธิภาพของมาตรการรักษาความปลอดภัยเขาจะรับรู้ได้ว่ามาตรการรักษาความปลอดภัยนั้นสามารถที่จะช่วยพวกเขาให้หลีกเลี่ยงภัยคุกคามได้

5.4.3.2 การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคาม ส่งอิทธิพลทางตรงต่อความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.150 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.033 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 4 ที่กล่าวว่า การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคามส่งผลเชิงลบถึงการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) ที่กล่าวว่า ผู้ใช้งานจะรับรู้ว่าเขาสามารถที่จะหลีกเลี่ยงภัยคุกคามได้เมื่อเขารับรู้ถึงค่าใช้จ่ายที่เกี่ยวข้องว่ามีค่าน้อยกว่าประโยชน์ที่เขาได้รับ ดังนั้น เมื่อค่าใช้จ่ายน้อยกว่าผลประโยชน์ผู้ใช้งานก็จะรับรู้ถึงความสามารถในการหลีกเลี่ยงและและมีแนวโน้มที่จะใช้มาตรการรักษาความปลอดภัยเหล่านั้น

5.4.3.3 การรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม ส่งอิทธิพลทางตรงต่อความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.264 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.000 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 5 ที่กล่าวว่า การรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคามส่งผลเชิงบวกถึงการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ซึ่งสอดคล้องกับงานวิจัยของ Maddux and Rogers (1983) และ Liang and Xue (2009) ที่กล่าวว่า ผู้ใช้งานจะรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามก็ต่อเมื่อเขารับรู้ถึงประสิทธิภาพของตนเองที่จะรับมือกับภัยคุกคามที่เกิดขึ้น หากผู้ใช้งานมั่นใจว่าเขาจะสามารถใช้มาตรการรักษาความปลอดภัยในการรับมือกับภัยคุกคามได้ เขาก็จะรับรู้ว่าเขาสามารถที่จะหลีกเลี่ยงภัยคุกคามได้

5.4.4 ผลการวิเคราะห์ตัวแปรอิสระที่ส่งผลถึงความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่

จากผลทางสถิติแสดงให้เห็นว่า การรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคาม การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคาม การรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม การรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม การรับรู้ถึงความรุนแรงของภัยคุกคาม และความกังวลในด้านความเป็นส่วนตัว ส่งอิทธิพลต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 33.0 ($R^2 = 0.330$) ซึ่งมีรายละเอียดในแต่ละปัจจัยดังนี้

5.4.4.1 การรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ส่งอิทธิพลทางตรงต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.222 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.001 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 6 ที่กล่าวว่า การรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ส่งผลเชิงบวกถึงความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ ซึ่งสอดคล้องกับงานวิจัยของ Claar (2011) และ Ng et al. (2009) ที่กล่าวว่า การรับรู้ภัยถึงคุกคามทำให้อุบัติการณ์เกิดความตั้งใจในการที่จะป้องกันตัวเองเพื่อหลีกเลี่ยงจากภัยอันตรายต่าง ๆ ได้ เมื่อบุคคลรับรู้ถึงภัยอันตรายที่จะเกิดขึ้นทำให้พวกเขามีความตั้งใจที่จะป้องกันภัยคุกคามนั้น ๆ

5.4.4.2 การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ส่งอิทธิพลทางตรงต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.508 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.000 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 7 ที่กล่าวว่า การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ส่งผลเชิงบวกถึงความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ ซึ่งสอดคล้องกับงานวิจัยของ Liang and Xue (2009) และ Steers et al. (2004) ที่กล่าวว่า การรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามสะท้อนถึงความสามารถในการใช้มาตรการรักษาความปลอดภัยของผู้ใช้งาน เมื่อผู้ใช้งานรับรู้ว่าเขาเองมีความสามารถที่จะหลีกเลี่ยงภัยคุกคามได้ก็จะเกิดความตั้งใจที่จะใช้มาตรการรักษาความปลอดภัยเพื่อที่จะป้องกันภัยคุกคามเหล่านั้นได้

5.4.4.3 การรับรู้ถึงประสิทธิผลของวิธีป้องกันภัยคุกคาม ส่งอิทธิพลทางอ้อมต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.110 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.4 การรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคาม ส่งอิทธิพลทางอ้อมต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ -0.076 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.5 การรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคาม ส่งอิทธิพลทางอ้อมต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.134 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.6 การรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม ส่งอิทธิพลทางอ้อมต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.031 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.7 การรับรู้ถึงความรุนแรงของภัยคุกคาม ส่งอิทธิพลทางอ้อมต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.107 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.4.8 ความกังวลในด้านความเป็นส่วนตัว ส่งอิทธิพลทางอ้อมต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.063 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

5.4.5 ผลการวิเคราะห์ตัวแปรอิสระที่ส่งผลถึงการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่

จากผลทางสถิติแสดงให้เห็นว่า ความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ การรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ และการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ส่งอิทธิพลต่อการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ โดยมีความผันแปรของตัวแปรตามเท่ากับร้อยละ 18.5 ($R^2 = 0.185$) ซึ่งมีรายละเอียดในแต่ละปัจจัยดังนี้

5.4.5.1 ความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ ส่งอิทธิพลทางตรงต่อการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ที่ค่าสัมประสิทธิ์อิทธิพลเท่ากับ 0.430 อย่างมีนัยสำคัญทางสถิติที่ระดับ 0.000 ซึ่งสอดคล้องกับสมมติฐานการวิจัยที่ 8 ที่กล่าวว่า ความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ส่งผลเชิงบวกถึงการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ ซึ่งสอดคล้องกับงานวิจัยของ Steers et al. (2004) และ Liang and Xue (2009) ที่กล่าวว่า บุคคลมีแนวโน้มที่จะแสดงพฤติกรรมเมื่อเขาเกิดแรงจูงใจและความตั้งใจต่อพฤติกรรมนั้น ดังนั้นบุคคลที่มีความตั้งใจในการหลีกเลี่ยงภัยคุกคามมีแนวโน้มที่จะเลือกใช้มาตรการรักษาความปลอดภัยที่สามารถทำให้เขาหลีกเลี่ยงภัยคุกคามได้

ตารางที่ 2 ผลการวิเคราะห์ค่าสัมประสิทธิ์สหสัมพันธ์ทางตรงและทางอ้อมของตัวแปรแฝงในกรอบแนวคิดการวิจัย

ตัวแปรแฝง	R ²	ทิศทาง	ตัวแปรสังเกต																				
			มูลค่าตรงของตัวแปรแฝง																				
การเข้าถึงเว็บไซต์ตามเงื่อนไข สำหรับผู้ใช้คอมพิวเตอร์โน้ตบุ๊ก	0.185	ทางอ้อม	มูลค่าตรงของตัวแปรแฝง	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-		
			มูลค่าตรงของตัวแปรแฝง	0.430*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ความพึงพอใจในการใช้เว็บไซต์ ตามเงื่อนไขสำหรับผู้ใช้คอมพิวเตอร์โน้ตบุ๊ก	0.330	ทางอ้อม	มูลค่าตรงของตัวแปรแฝง	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
			มูลค่าตรงของตัวแปรแฝง	-	0.098*	0.222*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
การเข้าถึงเว็บไซต์ตามเงื่อนไข สำหรับผู้ใช้คอมพิวเตอร์โน้ตบุ๊ก	0.471	ทางอ้อม	มูลค่าตรงของตัวแปรแฝง	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
			มูลค่าตรงของตัวแปรแฝง	-	-	-	0.110*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
การเข้าถึงเว็บไซต์ตามเงื่อนไข สำหรับผู้ใช้คอมพิวเตอร์โน้ตบุ๊ก	0.178	ทางอ้อม	มูลค่าตรงของตัวแปรแฝง	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
			มูลค่าตรงของตัวแปรแฝง	-	-	-	0.217*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
ความพึงพอใจในการใช้เว็บไซต์ ตามเงื่อนไขสำหรับผู้ใช้คอมพิวเตอร์โน้ตบุ๊ก	0.088	ทางอ้อม	มูลค่าตรงของตัวแปรแฝง	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
			มูลค่าตรงของตัวแปรแฝง	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

*p < .05

6. สรุปผลการวิจัย

6.1 บทสรุป

ผลการวิจัยพบว่า ปัจจัยความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวมีอิทธิพลต่อความกังวลในด้านความเป็นส่วนตัวในเชิงบวก ส่วนปัจจัยที่มีอิทธิพลต่อการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่มากที่สุดคือ ปัจจัยการรับรู้ถึงความรุนแรงของภัยคุกคาม รองลงมาคือ ปัจจัยความกังวลในด้านความเป็นส่วนตัว และปัจจัยการรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม ตามลำดับ ส่วนปัจจัยที่มีอิทธิพลต่อการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ พบว่าการรับรู้ถึงประสิทธิภาพของตนเองในการป้องกันภัยคุกคามเป็นปัจจัยที่มีความสัมพันธ์เชิงบวกมากที่สุด รองลงมาคือ ปัจจัยการรับรู้ถึงประสิทธิภาพของวิธีป้องกันภัยคุกคาม ส่วนปัจจัยการรับรู้ถึงค่าใช้จ่ายของวิธีป้องกันภัยคุกคามเป็นปัจจัยที่มีความสัมพันธ์เชิงลบ ส่วนปัจจัยที่มีอิทธิพลต่อความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่มากที่สุดคือ ปัจจัยการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ซึ่งส่งผลเชิงบวกและมีอิทธิพลมากกว่าปัจจัยการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ส่วนปัจจัยความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่มีอิทธิพลต่อการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ในเชิงบวก

6.2 ข้อเสนอแนะในเชิงปฏิบัติ

ผู้ที่เกี่ยวข้องสามารถนำผลการวิจัยไปประยุกต์ใช้ในด้านการรักษาความปลอดภัยทั้งในส่วนของธุรกิจและส่วนบุคคลได้ โดยแยกเป็นมุมมองต่าง ๆ ดังนี้

1. ผู้ให้บริการสามารถนำผลการวิจัยซึ่งพบว่าปัจจัยความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่มีอิทธิพลต่อการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่มาเป็นเป้าหมายในการพัฒนาวิธีป้องกันภัยคุกคาม โดยการสร้างแรงจูงใจให้ผู้ใช้บริการเห็นถึงภัยอันตรายที่อาจเกิดขึ้น เช่น การกระตุ้นให้ผู้ใช้บริการเกิดความตั้งใจและวางแผนที่จะใช้แอปพลิเคชันในการป้องกันภัยคุกคาม เช่น การทำให้ผู้ใช้บริการเกิดความมั่นใจในตัวแอปพลิเคชันว่าสามารถช่วยปกป้องข้อมูลส่วนตัวได้เป็นอย่างดี และหากไม่มีการป้องกันที่ดีแล้วจะส่งผลกระทบต่อข้อมูลส่วนตัวที่ถูกจัดเก็บไว้ในตัวเทคโนโลยีสวมใส่อย่างไรบ้าง โดยอาจเน้นไปทางการเสนอประโยชน์ที่จะได้รับ ข้อดีของการมีระบบป้องกันที่มีคุณภาพ และฟังก์ชันการใช้งานที่ง่ายต่อผู้ใช้บริการ เพื่อส่งเสริมและกระตุ้นให้เกิดการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ ซึ่งสามารถทำให้เกิดแรงจูงใจและความตั้งใจในการหลีกเลี่ยงภัยคุกคามและนำไปสู่การหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่ได้อย่างมีประสิทธิภาพ

2. ผู้ใช้บริการเทคโนโลยีสวมใส่รวมถึงบุคคลใกล้ชิดสามารถนำผลการวิจัยซึ่งพบว่าปัจจัยความตั้งใจในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่มีอิทธิพลต่อการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่มาเป็นข้อมูลในการช่วยกันป้องกันภัยคุกคามที่อาจเกิดขึ้นทั้งกับตนเองและบุคคลใกล้ชิด โดยสามารถนำข้อมูลจากปัจจัยการรับรู้ถึงโอกาสที่จะเกิดภัยคุกคาม การรับรู้ถึงความรุนแรงของภัยคุกคาม และความกังวลในด้านความเป็นส่วนตัว เช่น การให้ความรู้เกี่ยวกับภัยคุกคามต่าง ๆ เช่น ไวรัส สปายแวร์ หรือการคุกคามจากแฮกเกอร์ว่าสามารถเข้ามาทำอันตรายต่อข้อมูลส่วนตัวในเทคโนโลยีสวมใส่ได้ ซึ่งส่งผลให้เกิดการรับรู้ถึงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่เพื่อสร้างแรงกระตุ้นให้ผู้ใช้บริการและบุคคลใกล้ชิดเกิดแรงจูงใจและความตั้งใจในการหลีกเลี่ยงภัยคุกคามนำไปสู่การหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวจากการใช้เทคโนโลยีสวมใส่เพื่อช่วยลดปัญหาที่เกิดจากภัยคุกคามทางเทคโนโลยีลงไปได้

3. องค์กรที่เกี่ยวข้องในด้านระบบการรักษาความปลอดภัยทางเทคโนโลยี สามารถนำข้อมูลจากปัจจัยการรับรู้ถึงประสิทธิภาพของวิธีป้องกันภัยคุกคาม เช่น การทำให้ผู้ใช้บริการรู้สึกมั่นใจเมื่อใช้งานแอปพลิเคชันป้องกันแล้วจะสามารถปกป้องข้อมูลส่วนตัวได้ ซึ่งส่งผลต่อการรับรู้ถึงความสามารถในการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวในเทคโนโลยีสวมใส่มาเพื่อพัฒนาเครื่องมือป้องกันให้มีประสิทธิภาพและสามารถสร้างประโยชน์ให้กับผู้ใช้บริการได้

6.3 ข้อเสนอแนะสำหรับงานวิจัยต่อเนื่อง

ผู้วิจัยขอเสนอแนะงานวิจัยต่อเนื่อง ดังต่อไปนี้

1. กลุ่มตัวอย่างที่จัดเก็บในงานวิจัยนี้เป็นกลุ่มตัวอย่างคนไทยทั้งหมด ซึ่งในต่างประเทศมีผู้ใช้งานที่ใช้อุปกรณ์เทคโนโลยีสวมใส่กันอย่างแพร่หลาย อาจมีความแตกต่างทางวัฒนธรรมในด้านการรับรู้ถึงภัยคุกคามต่าง ๆ ทำให้ผลลัพธ์ยังไม่อาจครอบคลุมถึงภัยคุกคามทางเทคโนโลยีต่าง ๆ ที่มีอยู่ทั่วโลกได้ ข้อเสนอแนะในงานวิจัยต่อเนื่องอาจมีการจัดเก็บข้อมูลกลุ่มตัวอย่างจากต่างประเทศเพื่อให้ครอบคลุมและนำผลไปใช้ได้อย่างสมบูรณ์

2. งานวิจัยครั้งนี้ยังมีปัจจัยที่ไม่สนับสนุนสมมติฐานการวิจัย คือ ปัจจัยความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวซึ่งส่งอิทธิพลในทิศทางตรงข้ามกับสมมติฐานการวิจัย ทั้งนี้อาจเกิดจากการที่ผู้ใช้งานส่วนใหญ่ไม่สนใจหรืออาจไม่เข้าใจในนโยบายคุ้มครองข้อมูลส่วนตัวของผู้ให้บริการตามที่ได้กล่าวไปในข้อ 5.4.1 ในงานวิจัยต่อเนื่องอาจต้องมีการศึกษาปัจจัยความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวอีกครั้ง เพื่อหาข้อสรุปของปัจจัยนี้ให้ชัดเจนมากขึ้น

3. งานวิจัยครั้งนี้ พบว่า ปัจจัยความกังวลในด้านความเป็นส่วนตัวมีความผันแปรของตัวแปรตาม (R^2) ระหว่างปัจจัยความโปร่งใสของนโยบายคุ้มครองข้อมูลส่วนตัวที่ส่งอิทธิพลต่อปัจจัยความกังวลในด้านความเป็นส่วนตัวค่อนข้างน้อย $R^2 = 0.068$ จึงควรศึกษาปัจจัยเพิ่มเติมที่มีอิทธิพลต่อปัจจัยความกังวลในด้านความเป็นส่วนตัว

บรรณานุกรม

- นิธิป ชวนตันติกมล. (2557). พฤติกรรมการหลีกเลี่ยงภัยคุกคามข้อมูลส่วนตัวภายใน Public Cloud. การค้นคว้าอิสระปริญญาโทบริหารธุรกิจ, มหาวิทยาลัยธรรมศาสตร์.
- ภาวรุช พงษ์วิทย์ภานุ. (2557). เทคนิคเจาะลึก บันทึก วิเคราะห์ ชีวิตคุณด้วย Wearable Device + LifeLog. ดึงข้อมูลวันที่ 3 กุมภาพันธ์ 2559 สืบค้นจาก <http://www.pawoot.com/Wearable-Device-and-LifeLog>
- Bandura, A. (1977). Self-Efficacy: Toward a Unifying Theory of Behavior Change. *Psychological Review*, (84), 191-215.
- Bandura, A. (1982). Self-Efficacy Mechanism in Human Agency. *American Psychologist*, (37), 122-147.
- Claar, C. L. (2011). The adoption of computer security: An analysis of home personal computer user behavior using the health belief model. *Utah State University*.
- Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research*, 17(1), 61-80.
- Dachis, A. (2012). Do You Read Privacy Policies and Do You Understand Them. Retrieved February 3, 2016, from <http://lifelifehacker.com/5964185/do-you-read-privacy-policies-and-do-you-understand-them>.
- Edwards, K. (2015). Examining the security awareness, information privacy, and the security behaviors of home computer users. *ProQuest Dissertations and Theses*, 160.
- Glanz, K., Rimer, B.K., & Viswanath, K. (2008). Health Behavior and Health Education: Theory. *Research and Practice* (4th).
- Hair, J. F., Black, W. C., Babin, B. J., Anderson R. E., & Tatham, R. L. (1998). Construct Validity and Reliability. Retrieved February 3, 2016, from <http://wallaby.vu.edu.au/adtVVUT/uploads/approved/adtVVUT20080416.115505/public/05Chapter4.pdf>
- Hughes, A. (2014). Threat assessment of wearable technology. *ProQuest Dissertations and Theses*, 42.
- Janz, N.K., & Becker, M.H. (1984). The Health Belief Model: A Decade Later. *Health Education Quarterly*, 11(1), 1-45.

- Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical perspective. *MIS Quarterly*, 33(1), 71-90.
- Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. *Journal of the Association for Information Systems*, 11(7), 394-413.
- Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology*, 19(5), 469-479.
- Manzano, D. L. (2012). The cybercitizen dimension: A quantitative study using a threat avoidance perspective. *ProQuest Dissertations and Theses*, 112.
- Mills, A. J., Watson, R. T., Pitt, L., & Kietzmann, J. (2016). Wearing safe: Physical and informational security in the age of the wearable device. *Business Horizons*, 59(6), 615.
- Ng, B., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support System*, 46(4), 815–825.
- Oliver, R. L., & Berger, P. K. (1979). A Path Analysis of Preventive Health Care Decision Models. *Journal of Consumer Research*, 6(2), 113-122.
- Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, 28(8), 816.
- Rosenstock, I. M. (1974). The Health Belief Model and Preventive Health Behavior. *Health education Monographs*, 354-386.
- Sim, I. (2010). Online information privacy and privacy protective behavior: How does situation awareness matter. *ProQuest Dissertations and Theses*, 177.
- Son, J., & Kim, S. S. (2008). Internet users' information privacy-protective responses: a taxonomy and a nomological model. *MIS Quarterly*, 32(3), 503.
- Steers, R. M., Mowday, R. T., & Shapiro, D. L. (2004). The Future of Work Motivation Theory. *Academy of Management Review*, 29(3), 379-387.
- Van , S. C., Shin, J. T., Johnson, R., & Jiang, J. (2006). Concern for information privacy and online consumer purchasing. *Journal of the Association for Information Systems*, 7(6), 415-431.
- Weinstein, N.D. (1993). Testing Four Competing Theories of Health-Protective Behavior. *Health Psychology*, 12(4), 324-333.