การศึกษาพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเตอร์เน็ต

บุศรินทร์ อันทะรินทร์[1] ,วันจักร น้อยจันทร์[2]
เมธี สูตรสุคนธ์[3] ประวีณา ชาดี[4]
[1]สาขาวิชาการบริหารงานตำรวจ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา , โทรศัพท์ 098-4387-994
[1]E-mail : goodningth@gmail.com

บทคัดย่อ

การวิจัยนี้ มีวัตถุประสงค์เพื่อ 1.ศึกษาถึงพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเตอร์เน็ต 2. เพื่อเปรียบเทียบ พฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตจำแนกตามปัจจัยส่วนบุคคล โดยกลุ่มประชากรที่ใช้ในการวิจัยในครั้งนี้คือ นักศึกษาระดับปริญญาตรี ภาคปกติ คณะมนุษยศาสตร์และสังคมศาสตร์ สาขาวิชารัฐประศาสนศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทาชั้นปีที่ 1 – 4 จำนวน 292 คน ซึ่งได้นำมาแบ่งแบบสะดวกและเจาะจง ทำการวิเคราะห์ข้อมูลโดยใช้สถิติ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน t-test และ f-test (one way ANOVA) ระยะเวลาที่เริ่มศึกษาตั้งแต่เดือน 21 มกราคม 2562 ถึง วันที่ 30 เมษายน 2562 ส่วนระยะเวลาที่ใช้ในการศึกษารวม 3-4 เดือน

ผลการศึกษาพบว่า

กลุ่มตัวอย่างมีระดับการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตอยู่ในระดับ มากที่สุด ($\bar{x}$=4.36, S.D.=0.686) เมื่อพิจารณาเป็นรายข้อพบว่ากลุ่มตัวอย่างไม่ใช้รูปภาพวาดหวิวโพสลงทางสื่อออนไลน์มากที่สุด ($\bar{x}$=4.99, S.D.=0.101) รองลงมาเป็นใช้แอคเคาท์โซเชียลมีเดีย โซเชียลเน็ตเวิร์ก เช่น เฟสบุ๊ค ไลน์ อินสตาแกรม ทวิตเตอร์ เป็นการติดต่อสื่อสาร ($\bar{x}$=4.69, S.D.=0.599) ส่วนน้อยที่สุดคือ ใช้สั่งของทางออนไลน์ ($\bar{x}$=4.02, S.D.=0.855) และ กลุ่มตัวอย่างที่มี เพศ ชั้นปี ระยะเวลาที่ใช้โทรศัพท์มือถือ แตกต่างกัน มีพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตไม่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 และกลุ่มตัวอย่างที่มีประเภทการใช้สื่อ โซเชียลเน็ตเวิร์ค แตกต่างกันอย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 เมื่อเปรียบเทียบรายคู่ พบว่ากลุ่มตัวอย่างที่มี การใช้สื่อโซเชียลเน็ตเวิร์คประเภท เฟสบุ๊คมีพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตมากกว่ากลุ่มตัวอย่างที่มี การใช้สื่อโซเชียลเน็ตเวิร์คประเภทไลน์ อย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 และ กลุ่มตัวอย่างที่มี การใช้สื่อโซเชียลเน็ตเวิร์คประเภท เฟสบุ๊คมีพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตมากกว่ากลุ่มตัวอย่างที่มี การใช้สื่อโซเชียลเน็ตเวิร์คประเภทอินสตาแกรมอย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05

คำสำคัญ : พฤติกรรม, การป้องกัน, การโจรกรรมข้อมูลทางอินเตอร์เน็ต

Title Use TH SarabunPSK Bold Font, Font Size 20.

Busarin Auntharin[1],Wanchak Noichan[2]

[1] Department of Police Administration Faculty of Humanities and Social Sciences Suan Sunandha Rajabhat University, Tel. 098-4387-994 [1]E-mail : goodningth@gmail.com

Abstract

The purpose of this research was to Studying the behavior of internet data theft prevention And for comparison Internet theft prevention behavior classified by personal factors In which the population used in this research is Normal undergraduate students, Faculty of Humanities and Social Sciences Department of Public Administration Suan Sunandha Rajabhat University, Year 1 - 4, a total of 292 people, which were divided into convenient and specific. Data were analyzed using statistics, mean, standard deviation, t-test and f-test (one way ANOVA). The duration of the study was from January 21, 2019 to April 30, 2019. The total duration of the study was 3. -4 months

The study indicated that

The sample group had the highest level of internet theft prevention ($\bar{x}$ = 4.36, SD = 0.686). When considering in each item, it was found that the samples did not use dizzy pictures posted on online media ($\bar{x}$ = 4.99, SD = 0.101), followed by social media accounts Social networks such as Facebook, LINE, Instagram, Twitter are communication ($\bar{x}$ = 4.69, S.D. = 0.599). The smallest is The use of online orders (=x = 4.02, SD = 0.855) and the sample groups having different sex, year and time using mobile phones had no significant difference in the behavior of internet theft prevention. Statistically significant at the 0.05 level, and the sample group using the media type Social network Differences were statistically significant at the level of 0.05 when comparing pairs. Found that samples with Use of networked social media Facebook has more behavior to prevent internet theft than the sample group that has Using social network media types With statistical significance at the level of 0.05 and the samples with Use of networked social media Facebook has more behavior to prevent internet theft than the sample group that has The use of Instagram social media with statistical significance at the level of 0.05

Keywords :: behavior, prevention, internet theft

บทนำ

ในปัจจุบันเทคโนโลยีสารสนเทศและอินเทอร์เน็ตได้เข้ามามีบทบาทในการดำเนินชีวิตและกิจกรรมต่างๆของทุกคนทั่วโลกได้อย่างรวดเร็ว เป็นสิ่งที่ช่วยอำนวยความสะดวกในการติดต่อสื่อสารระหว่างบุคคลที่อยู่ห่างไกลกัน โดยการใช้เทคโนโลยีการสื่อสารเครือข่ายสังคมออนไลน์อย่างเช่นเฟซบุ๊ก ไลน์ นั้น สิ่งเหล่านี้ล้วนมีข้อดีคือเป็นการสร้าง ความสัมพันธ์ทางการสื่อสารในรูปแบบใหม่ที่ไม่ได้จำกัดเฉพาะแต่การสนทนาซึ่งกันและกันเท่านั้น แต่ยังเป็นการ สร้างความสัมพันธ์ระหว่างเพื่อน ลดช่องว่างทางระยะทางและเวลาเพราะทำให้เราได้พบเพื่อนใหม่รวมถึงเพื่อน เก่า ๆ ที่ไม่ได้ติดต่อกันเป็นเวลานาน ทำให้การสื่อสารง่ายและรวดเร็วมากขึ้น โดยไม่ใช่แค่การรู้จักกันในกลุ่มเล็ก ๆ เท่านั้น แต่ยังทำให้เกิดการสื่อสารกันครอบคลุมทั่วโลก นอกจากนี้ยังสามารถประยุกต์ใช้ในด้านอื่น ๆ เช่น ด้าน ธุรกิจ ด้านการศึกษาและด้านบันเทิง เป็นต้น แต่ในความสะดวกสบายนั้นก็สามารถนำมาซึ่งความไม่ปลอดภัยจากผู้ไม่ประสงค์ดีอย่างง่ายดายเช่นเดียวกัน (บุญทัศน์ ยังน้อย 2550) โดยจะมาในรูปแบบของการแฮ็คข้อมูล (Hacker) หรือที่เรียกว่าการโจรกรรมข้อมูลทางอินเตอร์เน็ต ซึ่งสิ่งเหล่านี้ล้วนสร้างความเสียหายแก่ข้อมูลส่วนบุคคลในเครื่องมือสื่อสารแต่ละชนิดซึ่งก่อให้เกิดปัญหาตามมาตั้งแต่สร้างความรำคาญต่อผู้ใช้งานจนรวมไปถึงสามารถสร้างมูลค่าความเสียหายเป็นมูลค่านับล้านบาท รวมไปถึงการใช้บริการเครือข่ายสังคมออนไลน์ต่างๆ สามารถสร้างผลกระทบให้แก่ผู้ใช้ได้อย่างง่ายดาย การแสดงออกซึ่งตัวตน รวมถึงข้อมูลส่วนตัวอาจมีการถูกละเมิดความ เป็นส่วนตัว การโจรกรรมข้อมูลหรือรูปภาพ การเปิดเผยข้อมูลที่ปราศจากการกลั่นกรองอาจส่งผลกระทบต่อสิ่ง ต่าง ๆ หรือบุคคลที่อ้างถึงหรือมีส่วนเกี่ยวข้องได้รับความเสียหายได้ (เลิศชาย สุธรรมพร 2541)

ทั้งนี้จากปัญหาดังกล่าวซึ่งนับวันจะทวีความรุนแรงขึ้นเรื่อยๆ เนื่องจากด้านความเร็วในการรับส่งข้อมูลผ่านอินเทอร์เน็ตพัฒนาไปกว่า สมัยก่อนมาก ทำให้การโจมตีจากผู้ไม่ประสงค์ดีเป็นไปได้อย่างรวดเร็ว ดังนั้นทางผู้วิจัยจึงมีความสนใจที่จะทำการศึกษาในปัญหาเหล่านี้ซึ่งเป็นสิ่งที่อยู่ใกล้ตัวเราทุกคน โดยทำการศึกษาถึงพฤติกรรมในการป้องกันการโจรกรรมข้อมูลทางอินเตอร์เน็ต เพื่อที่จะทำให้ทราบถึงวิธีการในการเลือกใช้วิธีป้องกันและหาแนวทางในการรักษาความปลอดภัยให้ดีที่สุด

วัตถุประสงค์ของการวิจัย

1.เพื่อศึกษาถึงพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเตอร์เน็ต

2.เพื่อเปรียบเทียบ พฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตจำแนกตามปัจจัยส่วนบุคคล

การทบทวนวรรณกรรม

แนวคิดทฤษฎีเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ

สมคิด พงษ์ชาติ (2546). ได้กล่าวถึงการรักษาความปลอดภัยของระบบสารสนเทศไว้ 3 ด้าน ดังนี้

1.1 การรักษาความปลอดภัยทางด้านกายภาพ (Physical Security) เป็นกลยุทธ์ที่กล่าวถึงการปกป้องบุคคล ทรัพย์สินที่จับต้องได้ และ สถานที่ทำงานจากภัยคุกคามที่ หลากหลาย เช่น ไฟไหม้การเข้ามาโดยไม่ได้รับอนุญาต หรือ ภัยธรรมชาติ

1.2. การรักษาความปลอดภัยในการติดต่อสื่อสาร (Communications security) กล่าวถึงการปกป้องสื่อต่างๆ เทคโนโลยีและข่าวสารที่ใช้ติดต่อสื่อสารภายในองค์กร และมีความสามารถในการใช้เครื่องมือนั้นเพื่อให้บรรลุวัตถุประสงค์ขององค์กรอีกด้วย

1.3. การรักษาความปลอดภัยทางด้านเครือข่าย (Network Security)

แนวคิดทฤษฎีเกี่ยวกับอาชญากรรมออนไลน์

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, สำนักงานสถิติแห่งชาติ. (2554a) ได้กำหนดแนวคิดไว้ ดังนี้

2.1. การโกงข้อมูล เป็นการกระทำของผู้มิหวังดีปล้นข้อมูลในระบบผ่านทางอินเทอร์เน็ตทำให้เกิดผลประโยชน์แก่ตนเองในทางมิชอบ

2.2 Hacker กับ Cracker มีความหมายเดียวกัน คือ "บุคคลผู้ซึ่งมีความรู้ความ เข้าใจ ในทางระบบคอมพิวเตอร์และอินเทอร์เน็ตเป็นอย่างดี

2.3 การลอบดักฟัง การดักฟังหรือดักข้อมูลเป็นการโจรกรรมข้อมูลบนระบบเครือข่ายอินเตอร์เน็ต ซึ่งผู้เป็นเจ้าของข้อมูลไม่มีโอกาสจะได้รู้เลยว่า ข้อมูลของตนซึ่งส่งไปตามสายในข่ายของอินเตอร์เน็ตได้ถูกโจรกรรม ซึ่งเป็นการโจรกรรมข้อมูลที่ง่ายกว่าในอดีต

2.4 Phishing คือ การโจมตีในรูปแบบของการปลอมแปลงอี-เมล์ (Email Spoofing) และทำ การสร้างเว็บไซต์ปลอม เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอีเมล์เปิดเผยข้อมูลทางด้าน การเงินหรือข้อมูลส่วนบุคคลอื่นๆ

.แนวคิดทฤษฎีเกี่ยวกับการรักษาความปลอดภัยของข้อมูล (กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, สำนักงานสถิติแห่งชาติ. 2554b)

3.1 การระบุตัวตน (Identification) ภายในระบบสารสนเทศนั้นต้องมีการระบุตัวตนภายในตัวระบบได้ ในการระบุตัวต้นนี้ เป็นขั้นตอนแรกก่อนจะเข้าถึงข้อมูลชั้นความลับ และเป็นพื้นฐานขั้นตอนต่อไปในการพิสูจน์ตัวตน (Authentication) และการพิสูจน์สิทธ์(Authorization)

3.2 การพิสูจน์ทราบตัวตน (Authentication) การที่ระบบจะบอกได้ว่าเมื่อผู้ใช้งานนั้นทำการเข้าระบบมาแล้วว่าชื่อผู้ใช้งานนั้นมี รหัสผ่านตรงกับชื่อผู้ใช้งานภายในระบบหรือไม่

แนวคิดทฤษฎีเกี่ยวกับการก่ออาชญากรรมผ่านอินเตอร์เน็ต

Halder, Debarati, Jaishankar, Karuppannan, & Jaishankar, K. (2012). ได้แบ่งเป็น 4 ลักษณะดังนี้

4.1. การเจาะระบบรักษาความปลอดภัยทางกายภาพ ได้แก่ ตัวอุปกรณ์และสื่อต่างๆ แอคเคาท์ข้อมูลส่วนตัว รูปภาพ ไฟล์เสียง บัญชีธนาคาร

4.2. การเจาะเข้าไปในระบบสื่อสารและการรักษาความปลอดภัยของซอฟต์แวร์ข้อมูล ต่างๆ

4.3. เป็นการเจาะเข้าสู่ระบบรักษาความปลอดภัยของระบบปฏิบัติการ

4.4. เป็นการเจาะผ่านระบบรักษาความปลอดภัยส่วนบุคคล โดยใช้อินเตอร์เน็ตเป็นช่องทางในการกระทำความผิด

แนวคิดทฤษฎีเกี่ยวกับประเภทอาชญากรรมทางคอมพิวเตอร์

Rogers, R. W. (1983). อาชญากรรมคอมพิวเตอร์เกิดขึ้นหลากหลายรูปแบบ ทั้งที่มีผลกระทบต่อชีวิต ระบบรักษาความปลอดภัย และระบบเศรษฐกิจ การกระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์แยกออกได้เป็น 3 ส่วน ส่วนแรกคือการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ส่วนที่สอง คอมพิวเตอร์เป็นวัตถุที่ถูกกระทำความผิด และส่วนที่สาม การใช้คอมพิวเตอร์หาประโยชน์โดยไม่ได้รับอนุญาติ

แนวคิดทฤษฎีเกี่ยวกับการวิเคราะห์ความเสี่ยงของเทคโนโลยีสารสนเทศ

กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร, สำนักกำกับการใช้เทคโนโลยีสารสนเทศ (Cartographer). (2551). ได้กล่าวถึงความเสี่ยงของเทคโนโลยีสารสนเทศ เกิดได้ 2 ทาง คือ อิทธิพลภายนอก (External Forces) และอิทธิพลภายใน (Internal Forces)

แนวคิดทฤษฎีเกี่ยวกับด้านการประเมินความเสี่ยง (Risk Assessment)

เลิศชาย สุธรรมพร. (2541). ได้กล่าวถึง การประเมินความเสี่ยงเทคโนโลยีสารสนเทศ การประเมินความเสี่ยงของเทคโนโลยีสารสนเทศก็เช่นเดียวกับการประเมินความเสี่ยง ประเภทอื่น ที่อาจวัดความเสี่ยงออกมาได้ 3 ส่วนคือ

1. ความเสียหายที่เป็นตัวเงิน
2. การสูญเสียเวลาและโอกาสทางธุรกิจหรืองาน
3. การสูญเสียส่วนตัวที่ก่อให้เกิดความอับอาย
4. **แนวคิดทฤษฎีเกี่ยวกับกฎหมายด้านความปลอดภัยของข้อมูลสารสนเทศ**
5. สำนักงานตำรวจแห่งชาติ. (2556). กฎหมายเทคโนโลยีสารสนเทศ (Information Law) หรือมักเรียกกันว่า กฎหมายไอที (IT Law) เสนอโดย กระทรวงวิทยาศาสตร์ เทคโนโลยี และสิ่งแวดล้อม และเห็นชอบให้คณะกรรมการเทคโนโลยีสารสนเทศแห่งชาติ (National Information Technology Committee) หรือที่เรียกโดยย่อว่า คณะกรรมการไอทีแห่งชาติ หรือ กทสช. (NITC) ทำหน้าที่เป็นศูนย์กลางและประสานงานระหว่างหน่วยงานต่าง ๆ ดำเนินการจัดทำกฎหมาย เทคโนโลยีสารสนเทศและกฎหมายอื่น ๆ ที่เกี่ยวข้อง ทั้งนี้ คณะกรรมการไอทีแห่งชาติหรือ กทสช. (NITC) ได้ แต่งตั้งคณะอนุกรรมการเฉพาะกิจ เพื่อยกร่างกฎหมายไอทีทั้ง 6 ฉบับ
6. โดยมอบหมายให้ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ (National Electronics and Computer Technology Center) หรือที่มักเรียกโดยย่อว่า "เนคเทค" (NECTEC) สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (National Science and Technology Development Agency) หรือที่เรียกโดยย่อว่า"สวทช." กระทรวงวิทยาศาสตร์เทคโนโลยี และสิ่งแวดล้อม
7. ในฐานะสำนักงานเลขานุการคณะกรรมการไอทีแห่งชาติทำหน้าที่เป็นเลขานุการในการยกร่างกฎหมายไอทีทั้ง 6 ฉบับ เนคเทค จึงได้เริ่มต้นโครงการพัฒนากฎหมายเทคโนโลยีสารสนเทศขึ้น เพื่อปฏิบัติตามนโยบายที่ได้รับมอบหมายจากรัฐบาลและคณะกรรมการไอทีแห่งชาติในการยกร่างกฎหมายไอทีทั้ง 6 ฉบับ ให้แล้วเสร็จคือ

1.กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ (Electronic Transactions Law)

2. กฎหมายเกี่ยวกับลายมือชื่ออิเล็กทรอนิกส์ (Electronic Signatures Law)

3. กฎหมายเกี่ยวกับการพัฒนาโครงสร้างพื้นฐานสารสนเทศให้ทั่วถึง และเท่าเทียมกัน (National Information Infrastructure Law)

4.กฎหมายเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคล (Data Protection Law)

5. กฎหมายเกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (Computer Crime Law)

6. กฎหมายเกี่ยวกับการโอนเงินทางอิเล็กทรอนิกส์ (Electronic Funds Transfer Law)

งานวิจัยที่เกี่ยวข้อง

การวิจัยศึกษาพฤติกรรมการป้องกันการโจรกรรมข้อมูลส่วนตัวทางออนไลน์ ผู้วิจัยได้ศึกษารวบรวมจากเอกสาร และผลงานวิจัยที่ เกี่ยวข้อง ดังนี้

ศราวุฒิ จันทะคัด (2554) ได้ทำการศึกษา การจัดการความปลอดภัยภายในเครือข่ายคอมพิวเตอร์ กรณีศึกษา : บริษัทแซนด์แอนด์ซอยล์อุตสาหกรรม จำกัด ผลการศึกษาพบว่า การกำหนด ตรวจสอบในเรื่องการใช้งานอินเทอร์เน็ตพบว่าโปรแกรมนี้สามารถสนับสนุน นโยบายนี้ได้ทั้งหมดไม่ว่าจะเป็นการบล๊อกการใช้งานเว็บไซต์ที่มีความเสียต่อความปลอดภัย ของระบบเครือข่าย สามารถทำงานได้มีประสิทธิภาพ โดยแบ่ง

ออกเป็น ลดช่องโหว่ที่เกิดจากการที่แฮกเกอร์เข้าผ่านพอร์ตอื่น ๆโดยที่ผู้ดูแลระบบไม่ได้เปิด ไว้ สามารถเปิดพอร์ตใช้งานได้ ว่าต้องการให้พอร์ตใดใช้งานได้ สามารถบล็อกเว็บไซต์ที่ผิดกฎหมาย ซึ่งตาม พ.ร.บ.กำหนดไว้ ช่วยจัดการแบนด์วิดท์ในเครือข่ายได้อย่างมีประสิทธิภาพ ช่วยจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ และสามารถดูได้ว่าผู้ใช้งานท่านได้เข้า เว็บไซต์ใดบ้าง เวลาเข้าใช้งาน สามารถทำ Load Balancer ได้ ในกรณีที่อินเทอร์เน็ตอีกหนึ่งเส้นใช้งานไม่ได้ (จะ อยู่ในหมวดการดำเนินธุรกิจอย่างต่อเนื่อง) สามารถจัดทำ Captive portal ได้ โปรแกรมนี้สามารถสนับสนุนกับนโยบายที่ทางผู้จัดทำโครงงานจัดทำขึ้นทุกข้อ จัดทำนโยบายการใช้งานระบบคอมพิวเตอร์และการเชื่อมต่ออินเทอร์เน็ต โปรแกรมที่สนับสนุนนโยบายนี้ ไม่สามารถตรวจจับไวรัสประเภท Phishing ที่มา กับอีเมล์ ได้ดีเท่าที่ควร

วิธีดำเนินการวิจัย

1. ประชากรและกลุ่มตัวอย่าง

ประชากรที่ใช้ในการศึกษาครั้งนี้ คือ นักศึกษาระดับปริญญาตรี ภาคปกติ คณะมนุษยศาสตร์และสังคมศาสตร์ สาขาวิชารัฐประศาสนศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา มีจำนวน 1,080 คน (ข้อมูล ณ วันที่ 21 มกราคม 2562)

กลุ่มตัวอย่าง ที่ใช้คือนักศึกษาระดับปริญญาตรี ภาคปกติ คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทา ครอบคลุมทุกชั้นปี โดยผู้วิจัยเลือกใช้วิธีการสุ่มตัวอย่างแบบเจาะจง (purposive sampling) โดยเก็บข้อมูลกับนักศึกษาระดับปริญญาตรี ภาคปกติ คณะมนุษยศาสตร์และสังคมศาสตร์ สาขาวิชารัฐประศาสนศาสตร์ มหาวิทยาลัยราชภัฏสวนสุนันทาชั้นปีที่ 1 – 4 จำนวน 292 คน โดยวิธีคำนวณหาขนาดของกลุ่มตัวอย่างที่ระดับความเชื่อมั่น 95% ของ Taro Yamane

2. เครื่องมือที่ใช้ในการศึกษา

การวิจัยครั้งนี้เป็นการวิจัยเชิงปริมาณใช้เครื่องมือในการเก็บข้อมูลคือ แบบสอบถามแบ่งเป็น 2 ตอน คือ ปัจจัยสวนบุคคลของผู้ตอบแบบสอบถาม และ ข้อมูลการป้องกันการโจรกรรมข้อมูลทาง*อินเทอร์เน็ต*

3.ขั้นตอนและวิธีการในการวิเคราะห์ข้อมูล

ผู้วิจัยดำเนินการเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง ข้อมูลที่ได้จากแบบสอบถามนำมาวิเคราะห์ข้อมูล

1. วิเคราะห์ข้อมูลเบื้องต้นเพื่ออธิบายลักษณะของกลุ่มตัวอย่าง โดยใช้สถิติบรรยาย ได้แก่ ค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐาน

2. การเปรียบเทียบ พฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตจำแนกตามปัจจัยส่วนบุคคลโดยใช้สถิติเชิงอนุมานได้แก่ t-test และ F-test (one-way ANOVA)

ผลการวิจัย

1.พฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ต

ตารางที่1 ผลการศึกษาพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ต

ตัวแปล	$\overline{x}$	SD	แปล
1.ท่านระมัดระวังการใช้แอพพลิเคชั่นโอนเงินออนไลน์ผ่านมือถือ	4.05	0.951	มาก
2.ท่านใช้แอคเคาท์โซเชียลมีเดีย โซเชียลเน็ตเวิร์ก เช่น เฟสบุ๊ค ไลน์ อินสตาแกรม ทวิตเตอร์ เป็นการติดต่อสื่อสาร	4.69	0.599	มากที่สุด
3.ท่านไม่ใช้รูปภาพวาดหวิวโพส ลงทางสื่อออนไลน์	4.99	0.101	มากที่สุด
4.ท่านคิดว่าอาชญากรรมทางโซเชียลมีโอกาสเกิดขึ้น	4.07	0.698	มาก
5.ท่านระวังการนัดเจอกับบุคคลที่พึ่งรู้จักผ่านทางสื่อออนไลน์	4.17	0.867	มาก
6. ท่านคิดว่าโอกาสการโดนล่อลวงไปก่อเหตุอาชญากรรมทางโซเชียล	4.51	0.730	มากที่สุด
7.ท่านระมัดระวังการสั่งของทางออนไลน์	4.02	0.855	มาก
รวม	4.36	0.686	มากที่สุด

การตารางที่ 1 การศึกษาพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตพบว่ากลุ่มตัวอย่างมีระดับการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตอยู่ในระดับ มากที่สุด ($\overline{x}$=4.36, S.D.=0.686) เมื่อพิจารณาเป็นรายข้อพบว่ากลุ่มตัวอย่างไม่ใช้รูปภาพวาดหวิวโพสลงทางสื่อออนไลน์มากที่สุด ($\overline{x}$=4.99, S.D.=0.101) รองลงมาเป็นใช้แอคเคาท์โซเชียลมีเดีย โซเชียลเน็ตเวิร์ก เช่น เฟสบุ๊ค ไลน์ อินสตาแกรม ทวิตเตอร์ เป็นการติดต่อสื่อสาร ($\overline{x}$=4.69, S.D.=0.599) ส่วนน้อยที่สุดคือ ใช้สั่งของทางออนไลน์($\overline{x}$=4.02, S.D.=0.855)

ตารางที่ 2. เปรียบเทียบพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตจำแนกตามปัจจัยส่วนบุคคลโดยใช้สถิติเชิงอนุมานได้แก่

ตัวแปร	$\overline{x}$	SD	t/F	Sig.	คู่ที่แตกต่าง
เพศ					
(1) ชาย	4.34	0.030	-0.591	0.555	-
(2) หญิง	4.37	0.037			
ชั้นปี					
(1) ปี 1	4.31	0.382	1.342	0.261	-
(2) ปี 2	4.39	0.456			
(3) ปี 3	4.40	0.332			
(4) ปี 4	4.29	0.475			
สื่อที่ใช้					
(1) เฟสบุ๊ค	4.46	0.225	2.403	0.050	(1) > (2)
(2) ไลน์	4.29	0.5255			(1) > (3)
(3) อินสตาแกรม	4.25	0.524			
(4) ทวิตเตอร์	4.37	0.325			
(5) ยูทูป	4.35	0.358			

ตัวแปร	$\overline{x}$	SD	t/F	Sig.	คู่ที่แตกต่าง
ระยะเวลาที่ใช้					
(1) 4-6 ชั่วโมง	4.32	0.468	2.132	0.121	-
(2) 6-8 ชั่วโมง	4.32	0.474			
(3) มากกว่า 8 ชั่วโมง	4.42	0.243			

จากตารางที่ 2 เปรียบเทียบพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตพบว่ากลุ่มตัวอย่างที่มี เพศ ชั้นปี ระยะเวลาที่ใช้โทรศัพท์มือถือ แตกต่างกัน มีพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตไม่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 และกลุ่มตัวอย่างที่มีประเภทการใช้สื่อโซเชียลเน็ตเวิร์ค แตกต่างกันอย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 เมื่อเปรียบเทียบรายคู่ พบว่ากลุ่มตัวอย่างที่มี การใช้สื่อโซเชียลเน็ตเวิร์คประเภท เฟสบุ๊คมีพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตมากกว่ากลุ่มตัวอย่างที่มี การใช้สื่อโซเชียลเน็ตเวิร์คประเภทไลน์ อย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 และกลุ่มตัวอย่างที่มี การใช้สื่อโซเชียลเน็ตเวิร์คประเภท เฟสบุ๊คมีพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตมากกว่ากลุ่มตัวอย่างที่มี การใช้สื่อโซเชียลเน็ตเวิร์คประเภทอินสตาแกรมอย่างมีนัยสำคัญทางสถิติที่ระดับ 0.05

อภิปรายผล

การศึกษาพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตพบว่ากลุ่มตัวอย่างมีระดับการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตอยู่ในระดับ มากที่สุด เพราะในปัจจุบันมีการพัฒนาเทคโนโลยีสื่อสารอย่างรวดเร็วส่งผลให้มีผู้ใช้งานอินเทอร์เน็ตอย่างแพร่หลายทำให้ผู้ใช้งานต้องมีความระมัดระวังอย่างมากในการใช้งานหากถูกโจรกรรมข้อมูลทางอินเทอร์เน็ตจะก่อให้เกิดความเสียหายระดับสูงยากจะควบคุมได้ ซึ่งสอดคล้องกับการวิจัยเรื่องการปฏิบัติตามนโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศของพนักงานในระบบของบริษัท พัฒนาอสังหาริมทรัพย์ขนาดใหญ่รายหนึ่ง (ภัคพล จันทนวรานนท์ และเอกรินทร์ วิบูลย์ตั้งมั่น, 2560)

การเปรียบเทียบพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตพบว่ากลุ่มตัวอย่างที่มี เพศ ชั้นปี ระยะเวลาที่ใช้โทรศัพท์มือถือ แตกต่างกัน มีพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเทอร์เน็ตไม่แตกต่างกันอย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 และกลุ่มตัวอย่างที่มีประเภทการใช้สื่อโซเชียลเน็ตเวิร์คแตกต่างกันอย่างมีนัยสำคัญทางสถิติ ที่ระดับ 0.05 เพราะ ส่วนใหญ่สื่อเฟสบุ๊กเป็นสื่อที่มีความปลอดภัยต่ำและมีจำนวนผู้ใช้มากที่สุด และยังเปิดโอกาสให้คนทุกเพศทุกวัยเข้าถึงกันได้โดยง่ายทำให้เป็นช่องทางของมิจฉาชีพเข้ามาโจรกรรมข้อมูลทางอินเทอร์เน็ตได้โดยง่าย ดังนั้นผู้ที่ใช้เฟสบุ๊กจึงมีการป้องกันตนเองจากการการโจรกรรมข้อมูลทางอินเทอร์เน็ตอยู่ในระดับมากที่สุด ซึ่งสอดคล้องกับงานวิจัยเรื่องการตระหนักถึงความเป็นส่วนตัวด้านสารสนเทศบนเครือข่ายสังคมออนไลน์ ของนักศึกษาคณะอักษรศาสตร์ มหาวิทยาลัยศิลปากร กรณีศึกษาเฟซบุ๊ก (ผุสดี ดอกพรม, 2558) ซึ่งพบว่าในการใช้เฟสบุ๊กข้อมูลที่กลุ่มตัวอย่างเปิดเผยมากที่สุดคือ ข้อมูลสถาบันการศึกษา ข้อมูลวันเดือนปีเกิด และความสนใจ โดยข้อมูลเหล่านี้เป็นข้อมูลที่กลุ่มตัวอย่างใช้ในการพิจารณาเพิ่มเพื่อนหรือยอมรับค ร้องขอเพิ่มเป็นเพื่อนนอกจากนี้ยังพบว่ากลุ่มตัวอย่างตระหนักถึงความเป็นส่วนตัวด้านสารสนเทศบนเครือข่ายสังคมออนไลน์ในระดับมาก โดยเฉพาะประเด็นการมองเห็นข้อมูลจากผู้ไม่พึงประสงค์ กลุ่มตัวอย่างส่วนใหญ่ใช้กลยุทธ์การส่งข้อความส่วนตัวแทนการโพสต์บนไทม์ไลน์เพื่อไม่ให้

บุคคลที่ไม่ประสงค์เห็นข้อมูล อย่างไรก็ตามกลุ่มตัวอย่างส่วนใหญ่ยังไม่ค่อยตระหนักถึงนโยบายความเป็นส่วนตัวและการใช้ข้อมูลของเฟสบุ๊ก โดยเฉพาะอย่างยิ่งประเด็นการน าข้อมูลส่วนตัวและพฤติกรรมการใช้งานของผู้ใช้งานเฟสบุ๊กไปใช้ประโยชน์ทางการตลาด

ข้อเสนอแนะ

1.จากผลการวิจัยพบว่ากลุ่มตัวอย่างระมัดระวังการสั่งของออนไลน์น้อยที่สุด รองลงมาเป็นระมัดระวังการใช้แอพพลิเคชั่นโอนเงินออนไลน์ผ่านมือถือ ดังนั้นหน่วยงานที่เกี่ยวข้องควรต้องมีการประชาสัมพันธ์รณรงค์ให้ประชาชนเพิ่มความระมัดระวังการสั่งของออนไลน์และการใช้แอพพลิเคชั่นโอนเงินออนไลน์ผ่านมือถือมากขึ้น รวมทั้งหามาตรการป้องกันการโจรกรรมข้อมูลจากการสั่งของออนไลน์และการใช้แอพพลิเคชั่นโอนเงินออนไลน์ผ่านมือถือมากขึ้นด้วย

2.จากผลการวิจัยพบว่ากลุ่มผู้ใช้อินสตาแกรมมีการป้องกันตนเองจากการโจรกรรมข้อมูลทางอินเทอร์เน็ตน้อยที่สุดอย่างมีนัยสำคัญทางสถิติที่ระดับ0.05 ดังนั้นหน่วยงานที่เกี่ยวข้องควรต้องมีการประชาสัมพันธ์รณรงค์ให้ประชาชนเพิ่มความระมัดระวังการใช้อินสตาแกรมมากขึ้น รวมทั้งหามาตรการป้องกันการโจรกรรมข้อมูลจากการใช้อินสตาแกรมมากขึ้นด้วย

กิตติกรรมประกาศ

วิจัยเรื่องศึกษาพฤติกรรมการป้องกันการโจรกรรมข้อมูลทางอินเตอร์เน็ต สำเร็จลุล่วงได้ด้วยความกรุณาและคำแนะนำของอาจารย์วันจักร น้อยจันทร์ในการทำวิจัยในครั้งนี้ได้กรุณาเสียสละเวลา ตรวจสอบและแก้ไขให้วิจัยฉบับนี้มีความสมบูรณ์ และที่สำคัญที่สุดคืออาจารย์เมธี สูตรสุคนธ์การให้คำชี้แนะแนวทางการทำงานให้มีความเป็นระเบียบวินัย และมีความรับผิดชอบ ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูง ณ โอกาสนี้

ขอขอบพระคุณผู้ตอบแบบสอบถามที่ให้ความอนุเคราะห์ สละเวลาให้ข้อมูลที่สำคัญในการกรอกแบบสอบถามด้วยความมีน้ำใจและอัธยาศัยอย่างดียิ่ง

ขอขอบพระคุณครอบครัวและเพื่อนๆ รวมทั้งนางสาวประวีณา ชาดีและผู้ที่มีส่วนร่วมทุกท่านที่สนับสนุน และเป็นกำลังใจในการทำวิจัยฉบับนี้ให้สำเร็จลงด้วยดี ตลอดมาจนทำให้ผู้วิจัยประสบผลสำเร็จดั่งที่ตั้งใจ

เอกสารอ้างอิง

ให้เขียนเอกสารอ้างอิงตามรูปแบบ ระบบ APA (American Psychological Association) กรณีที่มีการอ้างอิงในส่วนเนื้อเรื่อง (citations in text) เพื่อระบุแหล่งที่มาของข้อมูล กำหนดให้ผู้เขียนบทความเขียนการอ้างอิงแบบนาม-ปี (name-year or author-date style) เป็นการอ้างอิงโดยระบุชื่อผู้แต่ง และปีพิมพ์ของเอกสาร ไว้ข้างหน้าหรือข้างหลังข้อความที่ต้องการอ้าง เพื่อบอกแหล่งที่มาของข้อความนั้น และมีการรวบรวมรายการเอกสารที่ใช้อ้างอิงทั้งหมดไว้ตอนท้ายเอกสาร เรียกว่า เอกสารอ้างอิง (references) โดยเรียงตามลำดับพยัญชนะภาษาไทย ยกตัวอย่าง เช่น

ผู้แต่ง. (ปี). **ชื่อเรื่อง.** สถานที่พิมพ์: สำนักพิมพ์.

ผู้แต่ง. (ปีที่พิมพ์). **ชื่อบทความ.** ชื่อวารสาร, ปีที่(ฉบับที่), เลขหน้า.

ผู้แต่ง. (ปี, เดือน). **ชื่อบทความ.** ชื่อวารสาร, ปีที่(ฉบับที่), เลขหน้า. สืบค้นเมื่อ เดือน วัน,ปี, จากฐานข้อมูล ชื่อฐานข้อมูล.

ผู้แต่ง. (ปี). **ชื่อเรื่อง.** สืบค้นเมื่อวัน เดือน, ปี, จาก ชื่อเว็บไซต์: URL

ตัวอย่าง

โพสต์ทูเดย์ (2558). **ข่าวรถเมล์สาย 8 ในตำนาน.** สืบค้น เมื่อ 14 สิงหาคม 2556, จาก http://www.posttoday.com/ analysis/report/240984)

มัณฑนา จงรักษ์. (2551). **สภาพความเป็นจริงและความคาดหวังของการใช้รถโดยสารประจำทางขององค์การขนส่งมวลชนกรุงเทพตามแนวคิดส่วนประสมการตลาดบริการ.** วิทยานิพนธ์รัฐประศาสนศาสตรมหาบัณฑิต สาขาวิชาการบริหารทั่วไป วิทยาลัยการบริหารรัฐกิจ มหาวิทยาลัยบูรพา.

วิเชียร ฮังนนท์. (2556). **ความคิดเห็นต่อคุณภาพการใช้บริการรถโดยสารประจำทางปรับอากาศองค์การขนส่งมวลชนกรุงเทพ เขตการเดินรถที่ 2.** วิทยานิพนธ์บริหารธุรกิจมหาบัณฑิต สาขาวิชาบริหารธุรกิจ มหาวิทยาลัยราชภัฏพระนคร.

Roscoe, J. T. (1975). Fundamental research statistics for the behavioural sciences. (2nd ed.). New York: Holt Rinehart & Winston.