หน่วยที่ 4
ความปลอดภัยยุคดิจิทัล

- คือ การเข้าใจความรู้พื้นฐานทั่วไปของความ ปลอดภัยบนโลกอินเทอร์เน็ต โดยจะมีอันตรายที่มาจากผู้ไม่ประสงค์ดีในโลก อินเทอร์เน็ต เครือข่ายสังคมออนไลน์ ได้อย่างถูกต้องและปลอดภัย เพื่อการ หลีกเลี่ยงภัยคุกคาม และรับมือกับภัยอันตรายในโลกดิจิทัล

ความมั่นคงปลอดภัยและความเป็นส่วนตัวทางดิจิทัล

ความมั่นคงปลอดภัยและความเป็นส่วนตัวทางดิจิทัล (Digital Security and Privacy)

เป็นศาสตร์ที่ว่าด้วยการสงวนรักษาไว้ซึ่งความลับความครบถ้วนถูกต้องความพร้อมใช้ของข้อมูลที่มีความสำคัญและการปกป้องข้อมูลส่วนตัวในโลกออนไลน์โดยอาศัยวิธีการตรวจสอบและประเมินความเสี่ยงของข้อมูลและระบบที่สำคัญและข้อมูลส่วนบุคคลที่เกี่ยวกับการใช้งานดิจิทัลและหาแนวทางในการตรวจสอบปกป้องและแก้ไขช่องโหว่รวมถึงภัยคุกคามที่ทำให้เกิดความเสี่ยงต่อชีวิตทรัพย์สินข้อมูลที่สำคัญข้อมูลส่วนบุคคลระบบและอุปกรณ์ดิจิทัลของผู้ใช้งานจากการกระทำโดยผู้ไม่ประสงค์ดีการกระทำที่ผิดพลาดของผู้ใช้งานหรือภัยธรรมชาติ

ความเป็นส่วนตัวทางดิจิทัล

ความเป็นส่วนตัวทางดิจิทัล (Digital Privacy)

คือสิทธิการปกป้องข้อมูลความส่วนตัวในโลกออนไลน์ของผู้ใช้งานที่บุคคลหรือหน่วยงานอื่นจะนำไปจัดเก็บนำไปใช้ประโยชน์หรือนำข้อมูลนั้นไปเผยแพร่ในปัจจุบันประเด็นด้านความเป็นส่วนตัวถือเป็นสิ่งหนึ่งที่ประชาชนเริ่มให้ความสำคัญเนื่องจากข้อมูลที่สามารถระบุถึงตัวตนและความเป็นส่วนตัวโดยข้อมูลส่วนบุคคลสามารถถูกนำไปใช้ได้ในหลายมิติตัวอย่างที่หนึ่งที่เห็นได้ชัดเจนคือ บริษัทบัตรเครดิตจะใช้ข้อมูลส่วนบุคคลในการยืนยันความเป็นตัวเราในการทำธุรกรรมผ่านทางโทรศัพท์เป็นต้น นอกเหนือจากนี้บริษัทที่ผลิตสินค้าและเจ้าของบริการยังสามารถนำข้อมูลส่วนบุคคลไปใช้ในการวิเคราะห์เพื่อทำการตลาดในการนำเสนอสินค้าและบริการให้กับประชาชนได้ ซึ่งทำให้เกิดความเสี่ยงที่ข้อมูลส่วนบุคคลจะถูกขโมยหรือนำไปใช้โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูล

รอยเท้าดิจิทัล (Digital Footprint)

เคยสังเกตหรือไม่ว่าเมื่อเปิดเว็บไซต์หนึ่งแล้วออกมาจะพบกับโฆษณาที่เกี่ยวข้องกับเว็บไซต์นั้นอยู่ในเว็บไซต์อื่นๆที่ผู้ใช้เข้าไปหรือแม้แต่การที่ผู้ใช้นำชื่อของผู้ใช้ไปค้นหาแล้วพบถึงเนื้อหาต่างๆที่อยู่ในผลการค้นหาสิ่งเหล่านี้ล้วนเกิดจากการนำร่องรอยข้อมูลที่ผู้ใช้ได้เคยกรอกข้อมูลที่เกี่ยวข้องกับตนเองลงไปในเว็บไซต์หรือบริการต่างๆ ในโลกออนไลน์ทั้งโดยสมัครใจและด้วยความบังเอิญหรือเกิดจากเจ้าของเว็บไซต์และบริการที่ผู้ใช้เคยเข้าถึงทำการเก็บข้อมูลการเข้าถึงของผู้ใช้ไว้หรือเกิดจากการเก็บข้อมูลการใช้งานของผู้ใช้โดยผู้ให้บริการอินเทอร์เน็ตซึ่งข้อมูลดังกล่าวถูกจัดเก็บไว้ให้เหลือเป็นร่องรอยของผู้ใช้อยู่บนอินเทอร์เน็ต โดยมีการเรียกข้อมูลเหล่านี้ว่า “รอยเท้าดิจิทัล” หรือ “Digital Footprint” รอยเท้าดิจิทัล นั้น สามารถเป็นได้ทั้งประโยชน์และโทษต่อผู้ใช้เองและผู้อื่นในส่วนประโยชน์ผู้ให้บริการเว็บไซต์สามารถใช้รอยเท้าดิจิทัลในการวิเคราะห์ความต้องการของผู้ใช้เพื่อการนำเสนอผลิตภัณฑ์และบริการที่ตรงกับ ความต้องการ หรือเพื่อแสดงผลการสืบค้นที่ใกล้เคียงกับความต้องการ ของผู้ใช้มากขึ้น

แนวทางการป้องกันและลดรอยเท้าดิจิทัล

ผู้ใช้สามารถป้องกันตนจากการสร้างรอยเท้าดิจิทัลได้ในหลายวิธีเช่นใชงานโปรแกรมกำจัดไวรัสคอมพิวเตอร์หรือ Add-onของเบราเซอร์ที่มีฟังก์ชันในการตรวจคัดกรองเว็บไซต์หรือบริการ Cloud ที่ไม่น่าเชื่อ อาทิ Add-on ชื่อ Web Of Trust (WOT) ที่ใช้ในการตรวจคัดกรองเว็บไซต์ที่ไม่น่าเชื่อถือ การตั้งค่าของแต่ละเบราว์เซอร์แล้วค้นหาคำว่า“ห้ามติดตาม” หรือ“Do Not Track”และเปิดคุณสมบัติดังกล่าวเพื่อจำกัดการติดตามผู้ใช้ ใช้งาน Add-onของเบราเซอร์ที่มีฟังก์ชันในการป้องกันการติดตามรอยเท้าดิจิทัล จากเว็บไซต์ที่ใช้งาน อาทิ Add-on ชื่อ Privacy Badger เป็นต้น Add-on Privacy Badger ที่ใช้ในการป้องกันการติดตามรอยเท้าดิจิทัล จากเว็บไซต์ที่ใช้งาน พิจารณาความเสี่ยงของการเกิดรอยเท้าดิจิทัลก่อนการโพสรูปหรือข้อความลงในเว็บไซต์ หรือสื่อออนไลน์ต่างๆ ตั้งค่าเพื่อควบคุมการติดตามรอยเท้าดิจิทัลในเว็บไซต์และสื่อออนไลน์ต่างๆ ผ่านทาง ระบบการจัดการความเป็นส่วนตัวของในแต่ละบริการ ซึ่งในระบบดังกล่าว ผู้ใช้สามารถ ควบคุมในกิจกรรมที่ผู้ให้บริการได้จัดเก็บไว้ในการเข้าใช้งานอินเทอร์เน็ตแต่ละครั้ง หากตรวจสอบพบว่ามีการละเมิดข้อมูลส่วนตัวให้เก็บหลักฐานที่พบพร้อมรายละเอียด ต่างๆ ที่เกี่ยวข้องแจ้งความที่สำนักงานตำรวจท้องที่หรือที่กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ

ความปลอดภัย ความมั่นคง (Security)

ความปลอดภัย ความมั่นคง (Security) เป็นศาสตร์ที่ว่าด้วยแนวทางการปกป้องระบบและอุปกรณ์ดิจิทัล จากการบุกรุกโดยผู้ใช้ภายนอกหรือจากความผิดพลาดของระบบที่เกิดจากผู้ใช้บริการ ความมั่นคงถือเป็นหนึ่งประเด็นที่ได้รับความสนใจทั้งภาคหน่วยงานและภาคประชาชน โดยในภาคหน่วยงานนั้น ต้องรับประกันว่าข้อมูลที่จัดเก็บภายในหน่วยงานมีความปลอดภัยเพียง พอที่จะสามารถรักษาความลับทางหน่วยงานรวมไปถึงข้อมูลลูกค้าของหน่วยงานได้ในส่วนภาคประชาชนนั้นควรที่จะคำนึงถึงความปลอดภัยเนื่องจากวิถีชีวิตในปัจจุบันนั้นเกี่ยวโยงกับเทคโนโลยีดิจิทัลเป็นอย่างมาก ประกอบกับข้อมูลส่วนบุคคลที่อยู่บนโลกออนไลน์มีปริมาณมากขึ้นทำให้ภาคประชาชนควรต้องรู้เรื่อง เกี่ยวกับความปลอดภัย เพื่อเป็นการป้องกันตัวเองจากผู้ไม่ประสงค์ดี

การพิสูจน์ตัวตน (Authentication)

การพิสูจน์ตัวตน (Authentication) เป็นกระบวนการที่ใช้ในการยืนยันว่าผู้ใช้ดังกล่าว เป็นเจ้าของข้อมูลที่ผู้ใช้ต้องการเข้าถึง โดยปัจจุบัน แนวทางการพิสูจน์ตัวตนมีหลากหลายวิธี โดยในกรณีนี้จะยกตัวอย่าง 2 วิธีที่เป็นที่นิยมในการเข้าถึงข้อมูล วิธีแรก เป็นวิธีการพิสูจน์ตัวบุคคลด้วยชื่อผู้ใช้และรหัสผ่าน (Username and Password) ซึ่งเป็นวิธีที่ได้รับความนิยมอย่างสูงมากในการเข้าถึงข้อมูลส่วนบุคคล วิธีที่สอง การพิสูจน์ตัวตนด้วยระบบสองปัจจัย (2-Step Authentication) เป็นแนวทาง ในการพิสูจน์ตัวตนที่เสริมความแข็งแรงจากการพิสูจน์ตัวตนด้วยชื่อผู้ใช้และรหัสผ่าน โดยวิธีดังกล่าว มีแนวทางในการพิสูจน์ตัวตนได้หลากหลายวิธี ประกอบด้วย วิธีการยืนยันตัวตนผ่านรหัสชั่วคราว วิธีการยืนยันตัวตนผ่านรหัสชั่วคราวที่ได้จากแอปพลิเคชันพิสูจน์ตัวบุคคล และระบบการยืนยันตัวตน ด้วยอุปกรณ์ที่ใช้เพื่อการยืนยันตัวตน แนวทางการยืนยันตัวตนผ่านรหัสชั่วคราว (One-time Password หรือ OTP) เป็นวิธีการ ยืนยันตัวตนที่อาศัยหมายเลขโทรศัพท์มือถือหรืออีเมลในการส่งข้อความพิเศษที่ใช้สำหรับการยืนยัน ตัวตนเท่านั้น

การเข้ารหัสข้อมูล

การเข้ารหัสข้อมูล (Encryption) เป็นวิธีการที่ทำให้ผู้ที่สามารถเข้าถึงข้อมูลได้โดยไม่ได้ รับอนุญาต เช่น การเข้าไปในระบบผ่านช่องโหว่ของระบบ (หรือการแฮ็ก) จะไม่สามารถอ่านข้อมูล ในรูปแบบปกติได้ เนื่องจากข้อมูลเหล่านั้นถูกแปลงโดยใช้ชุดแปลงข้อมูลที่สามารถอ่านได้เฉพาะคน ที่มีชุดแปลงข้อมูลนี้เท่านั้น การเข้ารหัสข้อมูลเริ่มได้รับความนิยมมากขึ้นเพื่อเป็นการรับประกันให้กับผู้ใช้ว่าข้อมูล ที่บันทึกเข้ามาในบริการหลายรายการจะไม่สามารถให้ผู้อื่นใช้งานข้อมูลเหล่านั้นได้ ซึ่งการเข้ารหัส ข้อมูลนั้ น มักจะใช้ในกรณีของข้อมูลที่มีความอ่อนไหวสูง เช่น ข้อมูลรหัสผ่าน หรือบทสนทนา ที่ต้องการความลับสูง รวมไปถึงการเข้าสู่เว็บไซต์ที่เน้นเรื่องธุรกรรมทางการเงิน

มัลแวร์ (Malware) และการโจมตี

Malicious Software (หรือเรียกสั้นๆ ว่า Malware) เป็นชื่อเรียกโดยรวมของซอฟต์แวร์ ที่ออกแบบมาเพื่อมุ่งร้ายต่ออุปกรณ์ดิจิทัล ข้อมูลส่วนตัวบนโลกออนไลน์ และเครือข่ายอินเทอร์เน็ต ส่วนมาก มัลแวร์มักจะใช้ในการโจมตีทางช่องทางดิจิทัล โดยประเภทของมัลแวร์และการโจมตีมี รายละเอียดดังต่อไปนี้ • **ไวรัส (Virus)** เป็นมัลแวร์ประเภทฝังตัว โดยอาศัยการส่งต่อจากเครื่องหนึ่งมาอีก เครื่องหนึ่ง โดยการแพร่กระจายนั้นจะอาศัยไฟล์หรือโปรแกรม และจะทำงานเมื่อ มีการเปิดใช้งานโปรแกรมหรือไฟล์เท่านั้น • **ม้าโทรจัน (Trojan Horses)** เป็นมัลแวร์ที่หลอกล่อให้ผู้ใช้หลงเชื่อว่าซอฟต์แวร์ ดังกล่าวปลอดภัย แต่สามารถสร้างความเสียหายเมื่อผู้ใช้หลงเชื่อไปติดตั้ง การทำงานจะคล้ายกับไวรัสแต่ผู้ใช้จะไม่ทราบว่ามีโปรแกรมที่ใช้มีโปรแกรมอื่นแฝง เข้ามาด้วย • **ประตูหลัก (Backdoors)** เป็นมัลแวร์ที่ใช้ช่องโหว่ของอุปกรณ์ในการเข้ามาใช้งาน อุปกรณ์โดยผู้ใช้ไม่รู้ตัว

มัลแวร์ (Malware) และการโจมตี

• **สปายแวร์ (Spyware)** เป็นมัลแวร์ที่สามารถดูพฤติกรรมการใช้งาน เช่น บัญชีผู้ใช้ รหัสผ่าน หรือข้อมูลทางการเงิน และส่งพฤติกรรมดังกล่าวไปยังผู้ไม่ประสงค์ดีเพื่อ ไปใช้ในทางไม่ถูกต้อง • **คีย์ล็อกเกอร์ (Keystroke logging)** เป็นมัลแวร์ที่คอยดักจับสิ่งที่ผู้ใช้พิมพ์เข้าไป ระหว่างใช้งานคอมพิวเตอร์ โดยสามารถอาศัยกับมัลแวร์ประเภทอื่นหรือแฝงตัวมา จากอุปกรณ์เสริมที่ใช้ร่วมกันกับอุปกรณ์ดิจิทัลได้ • **เวิร์ม (Worm)** เป็นมัลแวร์ที่สามารถกระจายตัวเองไปยังอุปกรณ์ดิจิทัลผ่านทาง เครือข่ายอินเทอร์เน็ต เช่น อีเมล์ ระบบเครือข่ายอินเทอร์เน็ต • **บอตเน็ต (Botnet)** เป็นการที่ผู้ไม่ประสงค์ดีนำอุปกรณ์ที่ติดมัลแวร์มาควบคุมเพื่อ สั่งการบางอย่าง ส่วนมากมักจะเป็นการนำอุปกรณ์ที่ติดมัลแวร์มาโจมตีกับ เป้าหมายเดียวกัน หรือใช้เพื่อทำการหาประโยชน์บางอย่างจากอุปกรณ์เหล่านั้น • **ซอฟต์แวร์เพื่อใช้ในการโฆษณา (Advertising Supported Software หรือ Adware)** เป็นซอฟต์แวร์เพื่อเป็นการโฆษณาผลิตภัณฑ์อื่นๆ โดยซอฟต์แวร์ ดังกล่าวมักจะมาพร้อมกับซอฟต์แวร์ติดตั้งอื่นๆ หรือโปรแกรมติดตั้งซอฟต์แวร์บางรายที่ได้รับโฆษณาจากซอฟต์แวร์บางเจ้า ส่วนมากซอฟต์แวร์เหล่านั้นมักจะสร้าง ความล าคาญให้กับผู้ใช้ อย่างไรก็ดี มีซอฟต์แวร์บางรายที่แฝงมัลแวร์อื่นๆ เข้ามา ด้วย • **รูทคิท (Rootkit)** เป็นมัลแวร์ที่ฝังเข้าไปในอุปกรณ์ดิจิทัลในระดับระบบปฏิบัติการ โดยมัลแวร์ประเภทนี้มีลักษณะคล้ายกับคีย์ล็อคเกอร์และบ็อตเน็ต กล่าวคือ มัลแวร์ตัวนี้จะเฝ้าสังเกตการณ์ กรองข้อมูล รวมถึงขโมยข้อมูล หรือใช้ทรัพยากร ของเครื่องเพื่อวัตถุประสงค์บางอย่าง เช่น การหารายได้จากการขุดสกุล เงินดิจิทัล (Cryptocurrency) ให้กับผู้ไม่ประสงค์ดีจากทรัพยากรของอุปกรณ์ดิจิทัลที่ ติดมัลแวร์

มัลแวร์ (Malware) และการโจมตี

• DoS - Denial of Service เป็นการโจมตีผู้ให้บริการผ่านการใช้ทรัพยากรของผู้ ให้บริการจนเกินพิกัดที่ผู้ให้บริการจะ รองรับได้ เพื่อขัดขวางไม่ให้ผู้ใช้รายอื่นเข้าใช้ งานบริการเหล่านั้นได้ ส่วนมากจะเป็นการโจมตีจากอุปกรณ์ที่ติดมัลแวร์บอตเน็ต • การหลอกลวงออนไลน์ (Fraud) เป็นช่องทางในการล่อลวงผู้ใช้ให้หลงเชื่อกับสิ่งที่ผู้ ไม่ประสงค์ดีตั้งใจที่จะหลอก ผู้ใช้ จนเกิดการเสียทรัพย์ หรือข้อมูลส่วนตัวเสียหาย เช่น การขายสินค้าที่ไม่มีอยู่จริงและเชิดเงินหนี หลอกล่อให้ผู้ใช้กรอก ข้อมูลส่วน บุคคล การปล่อยสัญญาณ Wi-Fi ปลอม เป็นต้น • ฟิชชิง (Phishing) คือการหลอกลวงประเภทหนึ่งที่อาศัย การสร้างเว็บไซต์ปลอม หรืออีเมล์ปลอม เพื่อหลอกล่อให้ผู้ใช้เข้าไปกรอกข้อมูลบัญชีผู้ใช้ หรือข้อมูลส่วนบุคคลของผู้ใช้ เช่น บัตรเครดิต โดยมีวัตถุประสงค์ที่จะสร้างความเสียหายทั้งด้าน ข้อมูลส่วนตัว และทรัพย์สิน • การโจมตีแบบวิศวกรรม สังคม (Social engineering) เป็นแนวทางการเสาะ แสวงหาข้อมูลของผู้ใช้จากการใช้รอยเท้าดิจิทัล เพื่อใช้เป็นแนวทาง หลอกล่อให้ ผู้ใช้ตกเป็นเหยื่อในการโจมตีด้วยวิธีอื่น ๆ • การหลอกลวง (Scam) เป็นแนวทางการหลอกล่อให้ผู้ใช้หลงเชื่อ เล่ห์อุบายที่ผู้ไม่ ประสงค์ดีได้หลอกล่อไว้ การหลอกลวงสามารถส่งผลกระทบถึงการทำงานของอุปกรณ์ดิจิทัลจากการ ฝังมัลแวร์เข้าไปในอุปกรณ์ หรือส่งผลต่อบัญชีของบริการ ดิจิทัลเพื่อนำไปใช้หลอกล่อผู้ใช้รายอื่นต่อไป

แนวทางการป้องกันด้านความปลอดภัย

ในปัจจุบัน การโจมตีผ่านช่องทางดิจิทัลเกิดขึ้นได้บ่อยขึ้นกว่าแต่ก่อนมาก การที่ผู้ใช้ทราบถึง แนวทางการป้องกันด้านความปลอดภัย เปรียบเสมือนกับการเสริมสร้างเกราะเพื่อพร้อมที่จะเผชิญหน้ากับผู้ไม่ประสงค์ดีที่จะอาศัยช่องโหว่ในการโจมตีได้ทุกเมื่อ สิ่งแรกที่ผู้ใช้ควรติดตัวไว้ก็คือ สติ เมื่อไรก็ตามที่ผู้ใช้เจอปัญหาที่เกี่ยวข้องกับความปลอดภัย เช่น บริการดิจิทัลที่ใช้อยู่โดนโจมตีให้ผู้ใช้เปลี่ยนรหัสผ่านในการเข้าใช้บริการเหล่านั้นทันที การใช้งาน อินเทอร์เน็ตผ่านโครงข่ายที่ไม่น่าไว้ใจ การเข้าชมเว็บไซต์ที่มีการเข้ารหัสแบบ HTTPS หรือการที่ผู้ใช้ คิดก่อนที่จะเข้าไปในเว็บไซต์บริการหรือไฟล์เอกสารที่มีโอกาสสูงที่จะทำให้ผู้ใช้ถูกโจมตีนอกจากนี้การตั้งรหัสผ่านที่ปลอดภัยก็เป็นอีกหนึ่งแนวทางที่สำคัญเช่นกัน โดยการที่จะตั้ง รหัสผ่านที่ดีได้นั้น ควรจะมีปัจจัยที่ต้องคำนึงถึงดังต่อไปนี้ ความยาวรหัสผ่านขั้นต่ำและ ขั้นสูงของผู้ให้บริการแต่ละราย ส่วนมากจะอยู่ที่ 8-16 ตัวอักษร รหัสผ่านไม่ควรจะเกี่ยวข้องกับข้อมูลส่วนตัว เช่น เบอร์ โทรศัพท์ วันเกิด หรือชื่อจริง และนามสกุล รหัสผ่านควรที่จะมีองค์ประกอบทั้ง ตัวเลข ตัวอักษรพิมพ์ใหญ่ ตัวอักษร พิมพ์เล็ก และอักขระพิเศษ รหัสผ่านควรมีความซับซ้อนมากพอ แต่ผู้ใช้ควรจะจดจ ารหัสผ่านได้ด้วยตนเอง **ควรที่จะลง ชื่อออกทุกครั้งเมื่อใช้บริการผ่านอุปกรณ์สาธารณะ**

ผลการวิเคราะห์การประยุกต์ความปลอดภัยยุคดิจิทัล ใช้กับชีวิตประจ าวัน

ความปลอดภัยและความเป็นส่วนตัวยุคดิจิทัลถือเป็นเรื่องหนึ่งที่ผู้อ่านควรให้ความสนใจ เนื่องจากปัจจุบัน ปัญหาด้านความปลอดภัยและความเป็นส่วนตัวอยู่ใกล้ตัวมากยิ่งขึ้น หนึ่งในปัญหาที่เกิดขึ้นและทำให้ประชาชนทั่วโลกสนใจเรื่องความเป็นส่วนตัวนั่นก็คือ กรณี ของเฟซบุ๊กกับบริษัทด้านการทำแผนการตลาดเชิงการเมือง Cambridge Analytica ได้มีการนำข้อมูลส่วนตัวของผู้ใช้บนเฟซบุ๊กไปใช้ในการวิเคราะห์เพื่อวางแนวทางการหาเสียงให้กับ Donald Trump ซึ่งต่อมาได้ขึ้นมาเป็นประธานาธิบดีของสหรัฐอเมริกา โดยเรื่องนี้ถูกเปิดโปงครั้งแรกโดยสำนัก ข่าว The Guardian ของสหราชอาณาจักร 4 สาเหตุสำคัญของปัญหานี้คือ เฟซบุ๊กเปิดให้นักพัฒนาเข้ามาพัฒนาซอฟต์แวร์เพื่อใช้ร่วมกับ เฟซบุ๊กเอง ซึ่งในช่วงนั้น ระบบการเชื่อมต่อของเฟซบุ๊กสามารถดึงข้อมูลส่วนตัวของผู้ใช้ได้ และทาง Cambridge Analytica ได้ใช้ช่องทางนี้ในการดึงข้อมูลส่วนตัวของผู้ใช้ผ่านการทำแบบสอบถามด้าน บุคลิกของแต่ละคน โดยข้อมูลที่ได้ไปนั้นมีตั้งแต่ ชื่อ สถานที่ วันเกิด เพศ รวมถึงการกด “ถูกใจ” เนื้อหาที่แบ่งปันบนเฟซบุ๊ก ทสามารถนำไปวิเคราะห์ข้อมูลของแต่ละบุคคลได้ และนำข้อมูลเหล่านั้น ไปใช้ในการวางแผนการหาเสียงเพื่อดึงดูดให้ประชาชนเลือก Donald Trump เป็นประธานาธิบดี จากเหตุการณ์ดังกล่าว ทำให้สังคมตั้งคำถามกับเฟซบุ๊กว่า เฟซบุ๊กมีวิธีการจัดการและรับประกันความเป็นส่วนตัวของผู้ใช้อย่างไร รวมไปถึงบริษัทเทคโนโลยีรายใหญ่ของโลกได้ออกมา ประนามเฟซบุ๊กเกี่ยวกับปัญหานี้ จนเกิดกระแสต่อต้านเฟซบุ๊กในระดับประชาชนด้วยการพิมพ์คำว่า #DeleteFacebook ในโพสต์บนสังคมออนไลน์อื่น อย่าง ทวิตเตอร์ เพื่อกระตุ้นให้ประชาชนร่วมกัน ปิดบัญชีเฟซบุ๊ก ซึ่งสะท้อนให้เห็นว่า ประชาชนเริ่มตระหนักถึงปัญหาด้านรอยเท้าดิจิทัล รวมถึง ปัญหาด้านความเป็นส่วนตัวที่เริ่มลดน้อยลงเรื่อยๆ และด้วยเหตุนั้นเอง ทำให้หลากหลายบริษัทที่ให้บริการด้านเทคโนโลยีดิจิทัลเริ่มมีแนว ทางการปกป้องความเป็นส่วนตัวของผู้ใช้มากขึ้น เช่น กูเกิลได้ปรับเปลี่ยนหน้าการตั้งค่าบัญชีเพื่อให้ สามารถควบคุมกิจกรรมได้ง่ายขึ้น แอปเปิลที่ชูเรื่องความเป็นส่วนตัวให้กับผู้ใช้ในทุกผลิตภัณฑ์

อ้างอิง

- http://miscenter.pcru.ac.th/regis-digital/
- **งานวิจัยและพัฒนาซอฟต์แวร์และเครือข่าย สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏเพชรบูรณ์**