ผลการบรรยายภัยคุกคามความมั่นคงทางไซเบอร์ในยุค Thailand 4.0

๑. ปัญหาความมั่นคงทางไซเบอร์เพิ่มจำนวนอย่างต่อเนื่องตามกระแสเทคโนโลยีเปลี่ยนโลก หรือ “Disruptive Technology” ซึ่งเป็นพัฒนาการของเทคโนโลยีที่มีความก้าวหน้า และมีอิทธิพลต่อการเปลี่ยนแปลงโลก สามารถเปลี่ยนรูปแบบการดำเนินชีวิต การประกอบธุรกิจ ทิศทางเศรษฐกิจโลก เช่น สิ่งต่างๆ ถูกเชื่อมโยงสู่โลกอินเทอร์เน็ต ทำให้มนุษย์สามารถสั่งการควบคุมการใช้งานอุปกรณ์ต่างๆ ผ่านทางเครือข่ายอินเทอร์เน็ต หรือที่เรียกว่า Internet of Things (IoT) หรือเทคโนโลยีหุ่นยนต์ที่เรียกว่าปัญญาประดิษฐ์ (Artificial Intelligence - AI) นอกจากนั้น การมีอิทธิพลเพิ่มขึ้นของเครือข่ายสังคมออนไลน์ โทรศัพท์เคลื่อนที่ประเภทสมาร์ทโฟน หรือ Cloud Computing Services ที่เป็นการให้บริการที่ครอบคลุมถึงการให้ใช้กำลังประมวลผล หน่วยจัดเก็บข้อมูล และระบบออนไลน์ต่างๆ แก่ผู้ใช้บริการทางอินเทอร์เน็ต ยิ่งก่อให้เกิดภัยคุกคามใหม่ๆ ทางไซเบอร์เพิ่มขึ้นในยุค Thailand 4.0

๒. ภัยคุกคามทางไซเบอร์ในปัจจุบันที่ส่งผลกระทบตั้งแต่ระดับบุคคล ขยายไปยังองค์กร จนถึงระดับความมั่นคงของชาติ ที่สำคัญและน่ากังวลอย่างยิ่งของไทย คือ ๑) การถูกชี้นำหรือครอบงำทางความคิดโดยไม่รู้ตัวจากเครือข่ายสังคมออนไลน์ และโทรศัพท์สมาร์ทโฟน ๒) การถูกละเมิดสิทธิความเป็นส่วนตัว (Privacy) ๓) การถูกขโมยข้อมูลไปใช้เพื่อวัตถุประสงค์ต่างๆ โดยเฉพาะด้านพาณิชย์ และ ๔) การได้รับข่าวสารลวง (Fake Information) โดยพบว่าบริษัทชั้นนำของโลกที่มีมูลค่าตามราคาตลาด (Market Capitalization) สูงสุด ๕ อันดับแรก ล้วนเป็นบริษัทที่ให้บริการเครือข่ายสังคมออนไลน์ ข้อมูลข่าวสาร และการให้บริการด้านการประมวลผล จัดเก็บข้อมูล และระบบออนไลน์ต่างๆ แก่ผู้ใช้บริการทางอินเทอร์เน็ต หรือ ระบบ Cloud Services อันได้แก่ เว็บไซต์ที่ให้บริการเครือข่ายสังคมออนไลน์ Facebook Youtube Line Microsoft และ Amazon ตามลำดับ ในด้านการข่าวกรอง วิทยากรเห็นว่า ข้อมูลข่าวสารที่ได้จากแหล่งข่าวเปิด (Open Source Intelligence - OSINT) จะมีความสำคัญอย่างมาก เพราะสามารถนำมาใช้ในการสร้างอิทธิพลทางความคิด และการสืบสวนหาเป้าหมายหรือข้อมูลผ่านทางไซเบอร์ ซึ่งปัจจุบันใช้กันแพร่หลายและมีแนวโน้มจะยิ่งใช้เพิ่มขึ้น

๓. ปัญหาภัยคุกคามทางไซเบอร์ที่น่ากังวลสำหรับไทยในปัจจุบันและในอนาคต คือ การถูกชี้นำหรือครอบงำทางความคิด โดยได้รับข้อมูลข่าวสารไม่ครบถ้วน และไม่รอบด้าน เพราะข้อมูลที่ได้เป็นข้อมูลที่ผู้ให้บริการวิเคราะห์จากข้อมูลในเชิงลึก และประสบการณ์การใช้อินเทอร์เน็ตของผู้ใช้ (User) ที่ถูกดึงมาจากระบบการจัดเก็บข้อมูล Cloud Services และโปรแกรมเครือข่ายสังคมออนไลน์ทั้งที่ผู้ใช้รู้ตัวและไม่รู้ตัวมาก่อน หรือที่เรียกว่า ปรากฏการณ์ “Filter Bubble Effect” กล่าวคือ ผู้ให้บริการจะเสนอแต่ข้อมูลที่ต้องการให้ผู้ใช้เห็น หรือให้ข้อมูลที่ตรงใจผู้ใช้เพราะผ่านการวิเคราะห์มาแล้ว ทำให้ผู้ใช้ไม่ได้รับข้อมูลที่ต้องการเห็นทั้งหมด เช่น กรณีการค้นหาข้อมูลในโปรแกรมค้นหา (Search Engine เช่น Google Yahoo) จากโทรศัพท์สมาร์ทโฟน หรือเครื่องคอมพิวเตอร์ นอกจากนั้น หากใช้สมาร์ทโฟนและเครื่องคอมพิวเตอร์เครื่องอื่นๆ ที่ต่างออกไปสำหรับค้นหาข้อมูลเดียวกัน จะเห็นว่า ผลลัพธ์ที่ได้จากการค้นหาก็จะแตกต่างกันไป เนื่องจากข้อมูลที่ปรากฏจะเป็นข้อมูลที่ผ่านการวิเคราะห์ผู้ใช้รายนั้นๆ ซึ่งมีแนวโน้มว่าเป็นข้อมูลที่นำเสนอให้แก่ผู้ใช้รายนั้นเพื่อให้ชอบหรือเห็นพ้องด้วย โดยที่ผู้ใช้จะไม่เห็น post หรือ comment ที่แตกต่างหรือขัดแย้งไปจากความคิดของผู้ใช้ ซึ่งยิ่งจะทำให้ผู้ใช้ไม่สามารถรับรู้ข้อเท็จจริงทั้งหมดที่อาจตรงข้ามกับผลลัพธ์ที่ผู้ใช้เห็นหรือได้รับ อันจะส่งผลต่อการตัดสินใจ ความเชื่อ ความคิด และความต้องการของผู้ใช้

๔. กรณีการได้รับข่าวสารลวงเพื่อวัตถุประสงค์ต่างๆ ตัวอย่างที่เห็นได้ชัด อาทิ กรณีการซื้อสินค้าในเว็บไซต์ออนไลน์ของ LAZADA กล่าวคือ หากผู้ใช้ดูราคาสินค้าชนิดใดไว้แต่ยังไม่ตัดสินใจซื้อ ผ่านไปอีก ๒ – ๓ วัน ผู้ใช้จะพบว่าราคาจะแพงขึ้นเมื่อเข้าดูเว็บไซต์ของ LAZADA อีกครั้ง อย่างไรก็ดี หากผู้ใช้เปลี่ยนเว็บเบราว์เซอร์แล้วเข้าดูราคาสินค้าตัวเดิม จะพบว่าราคาสินค้ายังคงเดิม ไม่ได้แพงขึ้น สถานการณ์นี้ยืนยันให้เห็นว่า ผู้ให้บริการเก็บและ

บันทึกข้อมูลความต้องการของผู้ใช้ แล้วทำการปรับราคาขึ้น เพื่อกระตุ้นการตัดสินใจ ทั้งนี้ การจัดการข้อมูล (Manipulate Data) ของผู้ให้บริการดังกล่าว ถือเป็นการสร้างอิทธิพลทางความคิด เบี่ยงเบนข้อมูล สร้างข้อมูลเท็จและลวงผู้ใช้ ซึ่งในกรณีนี้ปรากฏรายงานเมื่อ ๒๗ มิถุนายน ๒๕๖๐ ว่า สหภาพยุโรป (EU) สั่งปรับ Google เป็นเงิน ๒,๔๒๐ ล้านยูโร จากการชี้นำการเข้าใช้ Search Engine ของผู้ใช้ในทางที่ผิดในการใช้บริการสั่งซื้อสินค้าทางออนไลน์ ด้วยการทำราคาลวง

๕. การใช้สมาร์ทโฟน การค้นหาข้อมูล และการใช้โปรแกรมเครือข่ายสังคมออนไลน์ ล้วนก่อให้เกิดปัญหาอธิปไตยไซเบอร์ (Cyber Sovereignty) ที่สามารถกระทบถึงความมั่นคงแห่งชาติ การที่ผู้ใช้บันทึกข้อมูลหรือเข้าค้นหาข้อมูลในโปรแกรมค้นหา Search Engine เอื้อประโยชน์ต่อผู้ให้บริการมีข้อมูลของผู้ใช้โดยปริยาย และทำให้สามารถจัดเก็บข้อมูลตำแหน่งการใช้งาน (User Location) พฤติกรรมการค้นหาข้อมูล (User Search Behavior and Search Keyword) พฤติกรรมการเข้าชมภาพและวิดีโอ พฤติกรรมการซื้อสินค้าและบริการของผู้ใช้งาน เป็นต้น นำไปสู่การวิเคราะห์ข้อมูลเพื่อประโยชน์ด้านต่างๆ รวมถึงทางธุรกิจและการค้า โดยเฉพาะการที่ผู้ให้บริการล่วงรู้พฤติกรรมการใช้อินเทอร์เน็ตแล้วนำข้อมูลไปขายต่อ

๖. ปัจจุบันพบว่าบริษัทชั้นนำของโลกที่มีมูลค่าตามราคาตลาด (Market Capitalization) สูงสุด ๕ อันดับแรก ล้วนเป็นบริษัทที่ให้บริการเครือข่ายสังคมออนไลน์ และข้อมูลข่าวสาร ได้แก่ เว็บไซต์ Facebook Youtube Line Microsoft และ Amazon ตามลำดับ โดยมีบริษัท Alphabet เป็นบริษัทแม่ของ Google และ Youtube ซึ่งมีการแข่งขันทางธุรกิจแย่งความสนใจของมนุษย์ในแต่ละเรื่อง (Attention Span หรือเวลาเฉลี่ยที่มนุษย์ให้ความสนใจเสพสื่อข้อมูลข่าวสาร) โดยปี ๒๕๔๓ มนุษย์ใช้เวลาสนใจในแต่ละเรื่อง เฉลี่ย ๑๒ วินาที แต่คาดว่าในอนาคตมนุษย์ จะลดลงเหลือเพียง ๕ วินาที ซึ่งจะน้อยกว่าปลาทองที่มีความสนใจต่อสิ่งรอบข้าง ๙ วินาที อันเป็นผลให้สื่อต่างๆ ปรับวิธีการสื่อสารข้อมูลข่าวสารที่ต้องการในเครือข่ายสังคมออนไลน์ด้วยการดึงดูดความสนใจด้วยตัวอักษรสีแดง สั้นกระชับ และภาษาที่ดึงดูด เพื่อให้ผู้ใช้เมื่อเห็นการพาดหัวก็มักมีการแชร์ต่อ โดยยังไม่ได้อ่านเนื้อหาข่าว

๗. การใช้อินเทอร์เน็ตและสมาร์ทโฟนไม่ให้อยู่ในความควบคุมทางจิตใจของผู้ให้บริการ ผู้ใช้จึงต้องตระหนักว่าข้อมูลทั้งหมดที่ผู้ให้บริการรวบรวมและสามารถประมวลวิเคราะห์ได้นั้น เกิดจากตัวผู้ใช้เป็นผู้กรอกข้อมูลข่าวสารนั้นเมื่อผู้ใช้ทำการโหลดโปรแกรมต่างๆ การเข้าดูหรือค้นหาข้อมูล เป็นต้น ที่สำคัญข้อมูลที่ผู้ใช้ดำเนินการดังกล่าวไปแล้วจะไม่สามารถลบออกจากระบบได้ ทั้งนี้ แนวทางเบื้องต้นที่วิทยากรเสนอแนะ ได้แก่ ๑) การใช้โปรแกรมจับเวลาวัดสถิติการใช้งานสมาร์ทโฟนในชีวิตประจำวัน เช่น แอปพลิเคชัน Moment บนระบบ iOS ของไอโฟน และแอปพลิเคชัน Quality Time บนระบบ Android *(ผนวก ภาพ ๑)* ๒) การเข้าโปรแกรมเครือข่ายสังคมออนไลน์ เช่น เว็บไซต์ Facebook ต้อง Logout ทุกครั้ง เพราะการคง Login ไว้จะทำให้ระบบเก็บข้อมูลผู้ใช้ตลอดเวลา ควรลบหมายเลขโทรศัพท์เคลื่อนที่ และการตั้งค่าในเว็บไซต์ Facebook ในส่วนของ Timeline and Tagging ควรกำหนดให้ “เฉพาะฉัน” ที่สามารถ Post บนไทม์ไลน์ *(ผนวก ภาพ ๒)* ๓) การเข้า เว็บไซต์ Youtube หากไม่ต้องการให้ปรากฏวิดีโอที่ไม่ต้องการหรือไม่เหมาะสมทางด้านขวาของจอ ควรตั้งค่าด้านล่างด้วยการ click ปุ่ม Restricted Mode off ให้เป็น On *(ผนวก ภาพ ๓)* และ ๔) การใช้แอปพลิเคชัน Time Well Spent *(ผนวก ภาพ ๔)*

๘. การที่คนไทยมีแนวโน้มจะใช้สมาร์ทโฟนเพิ่มขึ้นอย่างมากและรวดเร็วนั้น สิ่งที่ควรตระหนักและต้องดำเนินการ คือ การเพิ่มทักษะความเข้าใจและการใช้เทคโนโลยีดิจิทัล (Digital Literacy) ให้เกิดประโยชน์สูงสุดในการสื่อสาร การปฏิบัติงาน และการทำงานร่วมกัน ในยุค S–M–C-I (Social – Mobile – Cloud – Information) ทั้งนี้ ผลวิจัยเมื่อพฤษภาคม ๒๕๖๐ พบว่าคนไทยใช้สมาร์ทโฟนกว่า ๑๓๐ ล้านเครื่อง และคนไทยใช้สมาร์ทโฟนเฉลี่ยวันละ ๖ ชั่วโมง ส่วน Mobile Application ที่นิยมใช้งานนานวันละหลายชั่วโมง ได้แก่ Facebook Youtube และ Line นอกจากนั้น คนไทยใช้ Facebook มากถึง ๔๗ ล้านบัญชี โดย ๔๖ ล้านบัญชีเป็นการใช้งานจากสมาร์ทโฟน ทั้งนี้

ปี ๒๕๖๐ มีผู้ใช้อุปกรณ์ IT ทั้งหมดในโลก ๒๕,๐๐๐ ล้านเครื่อง และคาดว่าภายในปี ๒๕๖๓ จะเพิ่มเป็น ๕๐,๐๐๐ ล้านเครื่อง อนึ่ง ไทยเป็นประเทศที่ถูกโจมตีทางไซเบอร์เป็นอันดับ ๕ ของเอเชีย และอันดับที่ ๑๑ ของโลก ขณะที่ อินเดีย อินโดนีเซีย และจีน เป็นประเทศที่ถูกโจมตีทางไซเบอร์มากที่สุดอันดับ ๑ ๕ และ ๘ ของเอเชีย

๙. แนวโน้มภัยคุกคามทางไซเบอร์ที่สำคัญนอกเหนือจากการถูกโจมตีทางไซเบอร์ คือ การถูกครอบงำและชี้นำทางความคิด และการถูกขโมยข้อมูล ทำให้ในอนาคตข้อมูลข่าวสารที่มาจากแหล่งข่าวเปิด (OSINT) จะก้าวขึ้นมามีความสำคัญอย่างมากในงานด้านข่าวกรองทั้งการวิเคราะห์ข้อมูล การสืบสวน และการปล่อยข่าวลวง โดยใช้บริษัทข้ามชาติที่มี Big Data (ข้อมูลจำนวนมากมายและมีรูปแบบที่หลากหลาย ไม่ว่าจะเป็นข้อความ รูปภาพ วิดีโอ มัลติมีเดีย) และมีนักวิทยาศาสตร์ข้อมูล (Data Scientist) ทำการประมวลและวิเคราะห์ข้อมูล และขายข้อมูลไปใช้ในวัตถุประสงค์ต่างๆ ทั้งด้านการเมือง การค้า และการก่อการร้าย เช่น บริษัท PALANTIR ซึ่งเป็นบริษัทให้บริการด้านข้อมูล โดยลูกค้าที่สำคัญ ได้แก่ สำนักงานข่าวกรองกลางสหรัฐฯ (CIA) สำนักงานความมั่นคงแห่งชาติสหรัฐฯ (NSA) สำนักงานสอบสวนกลางสหรัฐฯ (FBI) และกองทัพสหรัฐฯ ทั้งนี้ บริษัท PALANTIR เป็นผู้ให้เบาะแสชี้เป้าว่า โอซามะ บิน ลาดิน อยู่ที่ใดเมื่อปี ๒๕๕๔ และแจ้งแก่สิงคโปร์ถึงแผนการของกลุ่ม IS ในการจะตั้งจรวดที่เกาะบาตัม อินโดนีเซีย เพื่อโจมตีมารีนา เบย์ ของสิงคโปร์ เมื่อกรกฎาคม ๒๕๕๙ นอกจากนี้ยังมีบริษัทที่รับซื้อช่องโหว่หรือจุดอ่อนของซอฟท์แวร์และแอปพลิเคชัน ที่ทำให้ผู้โจมตีสามารถลดทอนความมั่นคงปลอดภัยของสารสนเทศของระบบใน Android และ iOS เช่น บริษัท Zerodium เป็นต้น

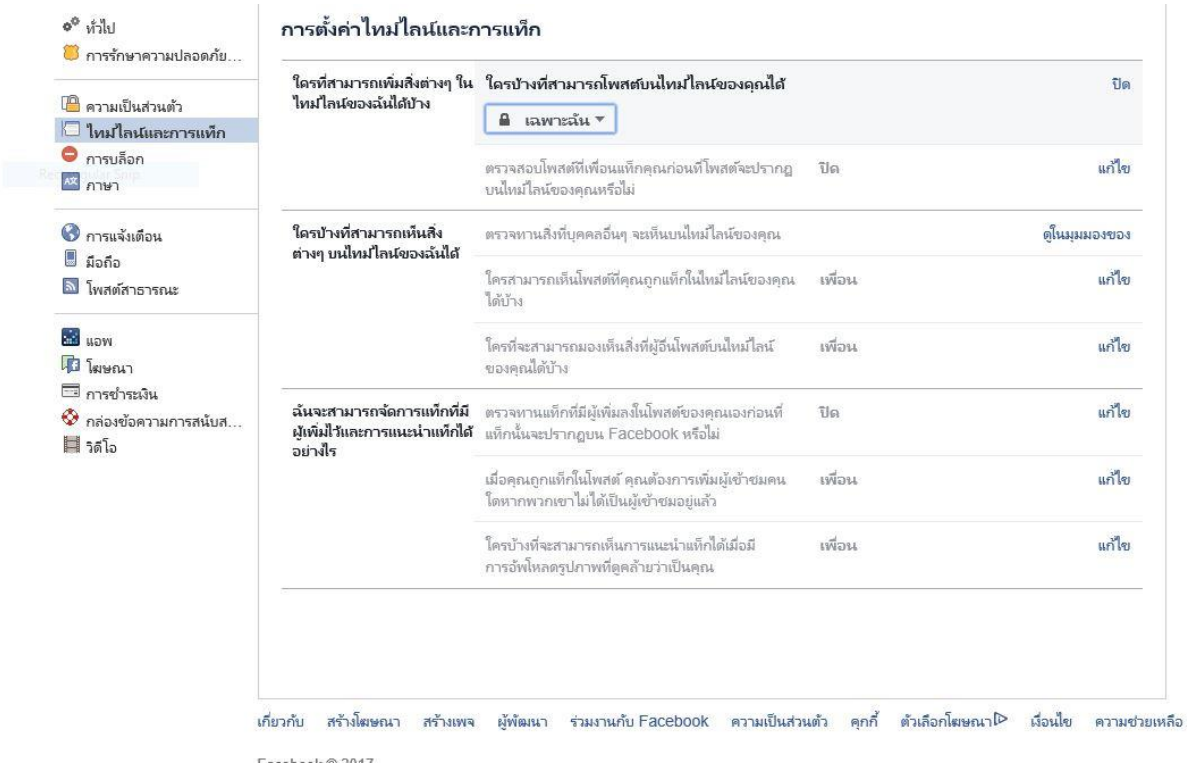
๑๐. สำหรับโปรแกรมหรือเว็บไซต์ที่ใช้ในการสืบสวนหาเป้าหมายหรือข้อมูลข่าวสาร วิทยากรชี้แนะว่ามีหลายโปรแกรมหรือเว็บไซต์ เช่น ๑) การดูความสัมพันธ์ของบุคคลเป้าหมายกับบุคคลอื่น กลุ่มบุคคล องค์กร บริษัท และอื่นๆ โดยเข้าไปที่เว็บไซต์บริษัท Paterva (www.paterva.com) ที่พัฒนาโปรแกรม Maltego (*ผนวก ภาพ ๕*) ๒) การค้นหาข้อมูลเบื้องต้น ได้แก่ อาหารที่ชอบ ครอบครัว ความฝักใฝ่ บรรพบุรุษ วันเกิด รถยนต์ที่ใช้ งานอดิเรกที่เว็บไซต์ Peekyou (www.peekyou.com *ดูผนวก ภาพ ๖)* และ ๓) การนำภาพในอดีตเพื่อหาแหล่งที่มาและอื่นๆ โดยใช้เครื่องมือ Exif *(*http://exif.regex.info *ดูผนวก ภาพ ๗)*

<u>ข้อพิจารณา</u>

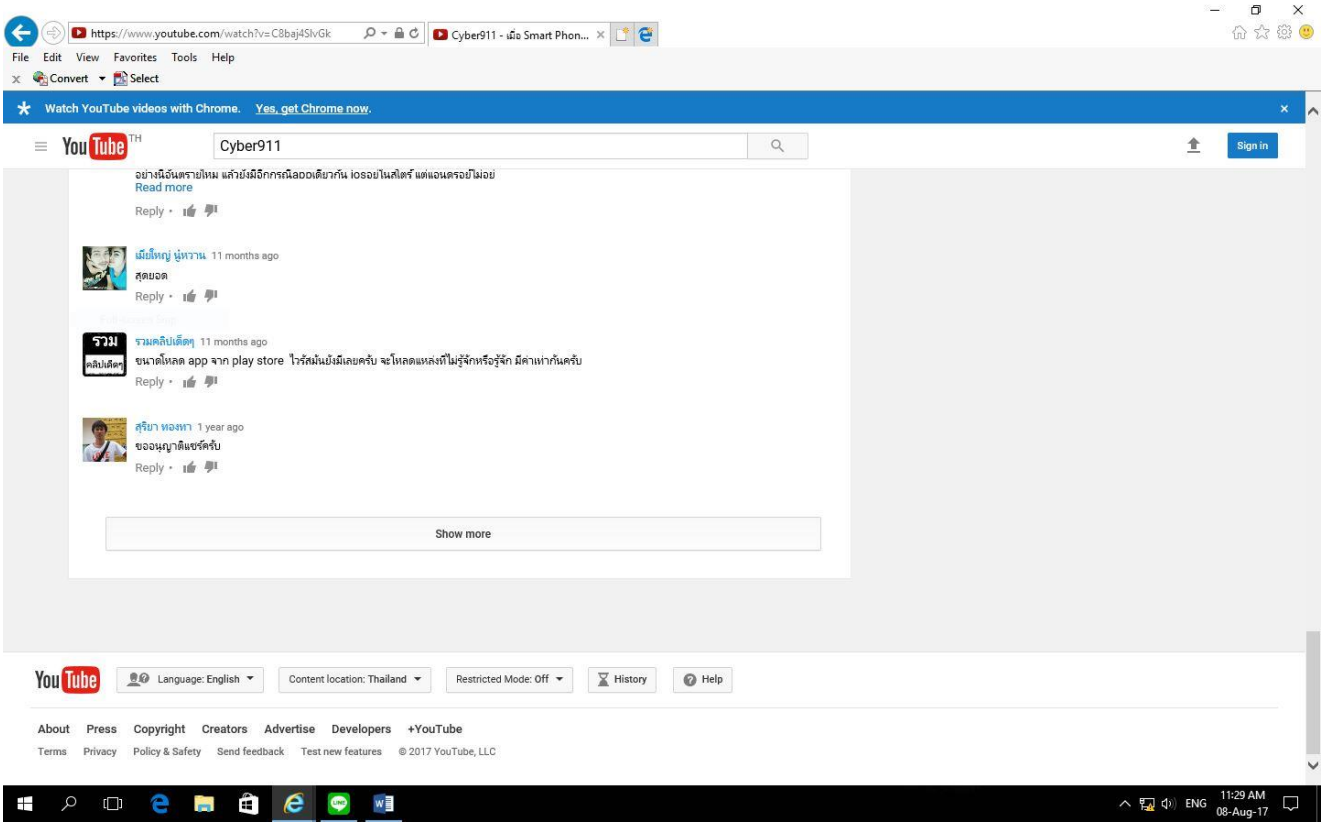
๑๑. วิทยากรให้ความเห็นว่า การใช้โทรศัพท์เคลื่อนที่ระบบ Android จะถูกบุคคลอื่นแฮกข้อมูลหรือเข้าระบบและเครือข่ายโดยไม่ได้รับอนุญาตได้ง่าย โดยเฉพาะในโทรศัพท์เคลื่อนที่ยี่ห้อ Oppo Samsung Lenovo ASUS และ Xiaomi ส่วนไอโฟนต้องปรับปรุงระบบให้เป็น iOS ๑๐.๓.๓ หากต่ำกว่านี้ มีความเสี่ยงถูกแฮกข้อมูลได้

๑๒. การบรรยายเรื่องภัยคุกคามความมั่นคงทางไซเบอร์ในยุค Thailand 4.0 เป็นประโยชน์ต่อหน่วยงานในประชาคมข่าวกรองในด้านการข่าว การระวังป้องกัน และยังเป็นเรื่องใกล้ตัวที่ทุกคนสามารถมีส่วนช่วยในการป้องกันภัยคุกคามทางไซเบอร์ ซึ่งนับวันยิ่งเป็นภัยคุกคามร้ายแรงทัดเทียมหรือมากกว่าภัยด้านอื่นๆ เช่น ภัยจากการก่อการร้าย ภัยคุกคามด้านนิวเคลียร์ เป็นต้น

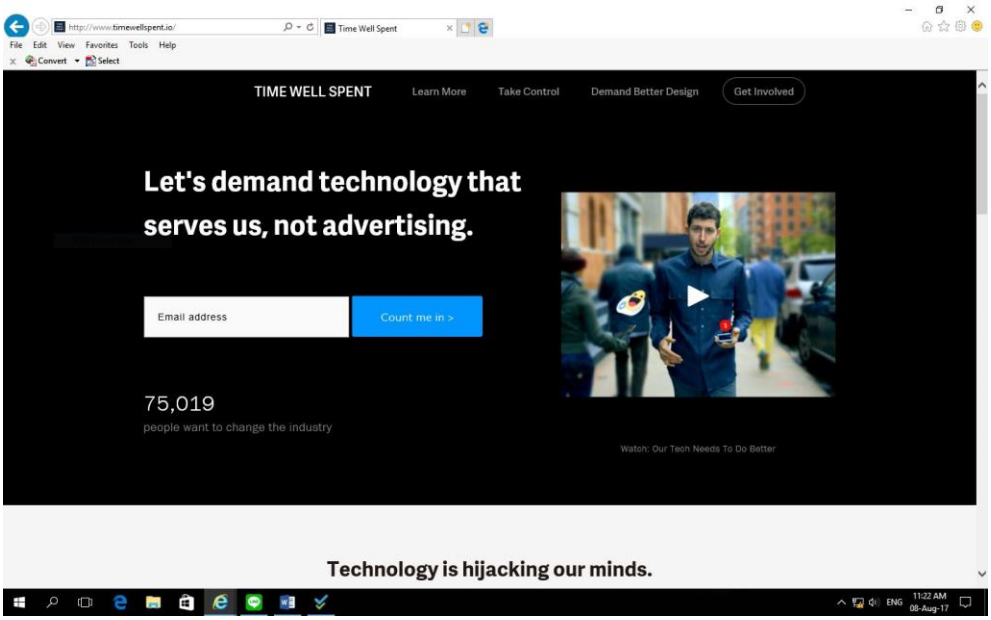
ภาพ ๑ โปรแกรม Moment บน iOS และ Quality Time บน Android



ภาพ ๒ การตั้งค่าใน Facebook ให้ระบุ เฉพาะฉัน ที่สามารถ Post บนไทมไลน์

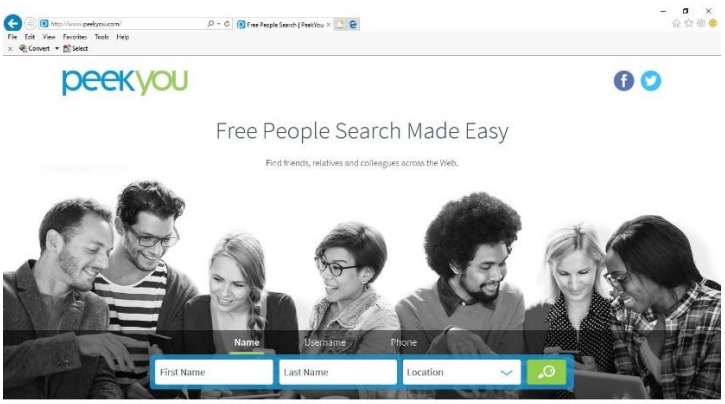


ภาพ ๓ เว็บไซต์ Youtube ให้กดปุ่ม Restricted Mode off ให้เป็น On

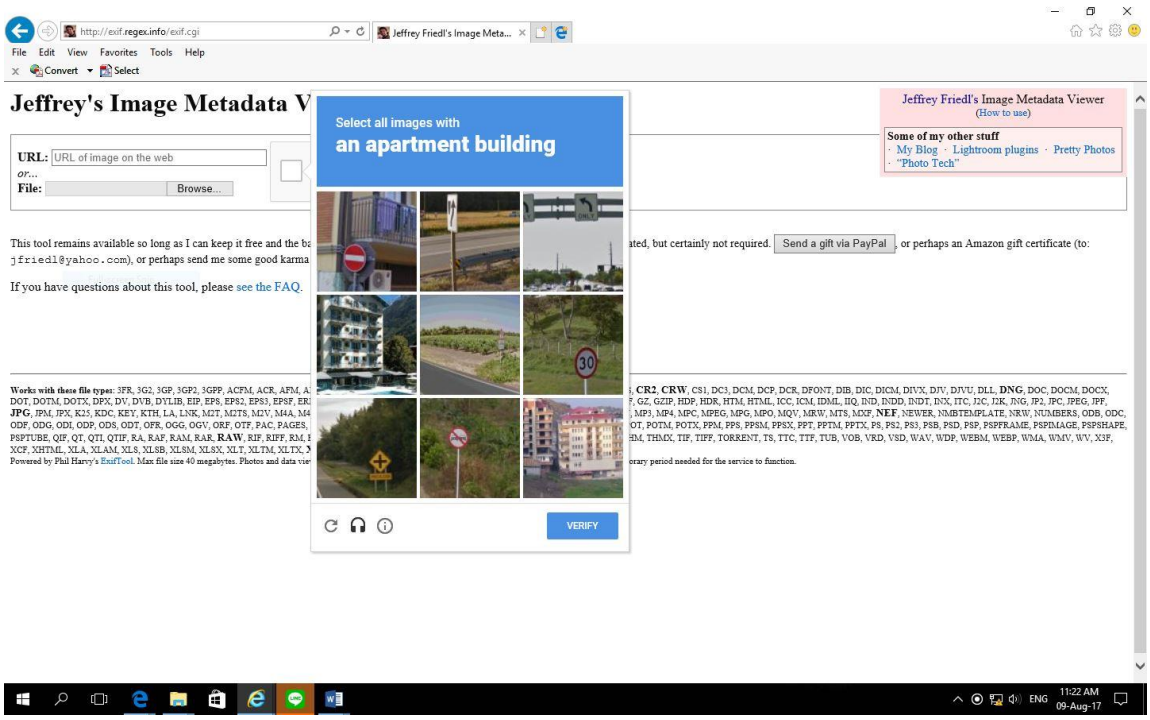


ภาพ ๔ แอปพลิเคชัน Time Well Spent http://www.timewellspent.io/

ภาพ ๕ เว็บไซต์บริษัท Paterva (https://www.paterva.com/web7) เพื่อจะใช้ Maltego หาความสัมพันธ์ของบุคคล



ภาพ ๖ เว็บไซต์ Peekyou (www.peekyou.com) หาข้อมูลเบื้องต้นของบุคคล



ภาพ ๗ การใช้ Exif (http://exif.regex.info) วิเคราะห์ภาพหาแหล่งที่มาและอื่นๆ