เอกสารเสนอบทความทางวิชาการ

เรื่อง

ความรู้ที่สำคัญด้านการรักษาความปลอดภัย สำหรับกำลังพลที่ใช้งานระบบสารสนเทศ

โดย

นาวาอากาศเอก ณัฐวุฒิ สามไพบูลย์

รองผู้อำนวยการกองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม
กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

พ.ศ.๒๕๖๑

บทคัดย่อ

กำลังพลกองทัพอากาศ ที่ใช้งานระบบสารสนเทศทั้งระบบและอุปกรณ์ของกองทัพอากาศ, ระบบและอุปกรณ์ส่วนบุคคลที่มีการเชื่อมต่อหรือใช้งานร่วมกับระบบและอุปกรณ์ของกองทัพอากาศ และการใช้งานเครือข่ายสังคมออนไลน์ของกำลังพล โดยภาพรวม ยังมีความรู้เกี่ยวกับภัยคุกคามและความตระหนักรู้ด้านการรักษาความปลอดภัยในการใช้งานระบบสารสนเทศทั้งมวลที่ไม่เพียงพอและไม่ครอบคลุม ซึ่งการยกระดับการรักษาความปลอดภัยแบบบูรณาการของกำลังพล ภายใต้ความรู้และความตระหนักรู้ที่ถูกต้องและเหมาะสม จะส่งผลให้ระดับของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศในภาพรวมสูงขึ้นและมีความปลอดภัยเพิ่มมากขึ้น

บทความทางวิชาการเรื่องความรู้ที่สำคัญด้านการรักษาความปลอดภัยสำหรับกำลังพลที่ใช้งานระบบสารสนเทศฉบับนี้ ได้มีการพิจารณาให้ครอบคลุมมิติสำคัญซึ่งกำลังพลควรทราบและเป็นประโยชน์ต่อการรักษาความปลอดภัยในการใช้งานระบบสารสนเทศอย่างบูรณาการ โดยได้ครอบคลุมองค์ความรู้เกี่ยวกับระบบสารสนเทศในด้านขององค์ประกอบที่เกี่ยวข้องและคุณสมบัติด้านความปลอดภัยของระบบสารสนเทศ รวมถึงภัยคุกคามทางไซเบอร์ทั้งรูปแบบเดิมและรูปแบบใหม่ที่พบปัจจุบัน พร้อมแนวทางในการป้องกัน

นอกจากนี้ ยังได้วิเคราะห์ถึงกำลังพลผู้ใช้งานระบบสารสนเทศ (Peopleware) กับการรักษาความปลอดภัยในมิติที่เกี่ยวข้องกับองค์ประกอบเชิงสารสนเทศอื่น, รหัสผ่าน (Password) และการพิจารณาความปลอดภัย ตลอดจนการตรวจสอบและยกระดับความปลอดภัยของรหัสผ่านที่ใช้งาน, การบูรณาการอุปกรณ์คอมพิวเตอร์และการสื่อสารส่วนบุคคลของกำลังพลมาใช้ร่วมกับระบบสารสนเทศของกองทัพอากาศ (BYOD) และการใช้บริการจัดเก็บข้อมูลบน Cloud Services กับการรักษาความปลอดภัย พร้อมทั้งได้แนะนำเทคโนโลยีด้านความปลอดภัยในปัจจุบันที่สำคัญและควรทราบ ได้แก่ การพิสูจน์ยืนยันตัวตนแบบพหุปัจจัย (Multi-factor Authentication), การลงลายมือชื่อดิจิทัล (Digital Signature) และเทคโนโลยี Blockchain ที่กำลังจะเข้ามาปฏิวัติรูปแบบการทำธุรกรรมอิเล็กทรอนิกส์แบบดั้งเดิม

พร้อมกันนี้ ได้เสนอแนะแนวคิด, แนวทาง และวิธีการในการกำหนดนโยบายด้านความปลอดภัยของหน่วยงานเพื่อยกระดับความปลอดภัย โดยยกตัวอย่างกรณีศึกษา Catch-Patch-Match ของ Australian Signal Directorate, Department of Defence ซึ่งเป็นตัวอย่างนโยบายด้านการรักษาความปลอดภัยอันทรงประสิทธิผลที่มีการประกาศเพื่อเป็นแนวทางกลยุทธ์ในการป้องกันภัยคุกคามทางไซเบอร์ให้กับทั้งองค์กรภาครัฐและเอกชนของประเทศออสเตรเลีย

ในส่วนท้าย ยังได้ประมวลองค์ความรู้ด้านกฎหมายที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่จำเป็นต้องระมัดระวังมิให้ละเมิดต่อกฎหมายในทุกมิติ ประกอบด้วย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐, พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ และ กฎหมายลิขสิทธิ์ พ.ศ.๒๕๕๘ นอกจากนี้ ยังได้สรุปประมวลจริยธรรมในการใช้งานระบบสารสนเทศที่มีความจำเป็นจะต้องปฏิบัติให้มีความเหมาะสม ถูกต้องตามทำนองคลองธรรม สอดคล้องกับวัฒนธรรม ประเพณี และมารยาทอันดีงามของสังคม ไว้ด้วย

คำนำ

กองทัพอากาศได้กำหนดวิสัยทัศน์ที่จะก้าวสู่ “กองทัพอากาศชั้นนำในภูมิภาค (One of the Best Air Forces in ASEAN)” ด้วยการเสริมสร้างสมรรถนะและความพร้อมของกำลังทางอากาศในการป้องกันประเทศ ภายใต้การเสริมสร้างนภานุภาพตามแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) และภายใต้ยุทธศาสตร์กองทัพอากาศ ๒๐ ปี (พ.ศ.๒๕๖๐ - ๒๕๗๙) ที่มุ่งเน้นการพัฒนาอย่างต่อเนื่อง โดยสร้างความเข้มแข็งในมิติไซเบอร์พร้อมกับวางรากฐานในมิติอวกาศเพื่อเตรียมความพร้อมในการป้องกันภัยคุกคามทุกรูปแบบที่จะเกิดขึ้นในอนาคต

ดังนั้น ความปลอดภัยในการใช้งานระบบสารสนเทศทั้งมวลจึงเป็นปัจจัยสำคัญที่จะส่งผลต่อความสำเร็จในการปฏิบัติภารกิจของกองทัพอากาศตามแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง

บทความทางวิชาการเรื่อง “ความรู้ที่สำคัญด้านการรักษาความปลอดภัยสำหรับกำลังพลที่ใช้งานระบบสารสนเทศ” ฉบับนี้ เขียนขึ้นจากความรู้และประสบการณ์ ภายใต้เจตนารมณ์ที่มุ่งหมายให้เป็นเอกสารประกอบในการเสริมสร้างความรู้และความตระหนักรู้ด้านการรักษาความปลอดภัยในการใช้งานระบบสารสนเทศแบบบูรณาการหลายมิติ ให้แก่กำลังพลของกองทัพอากาศ

สารบัญ

สารบัญตารางประกอบ

รายการ **หน้า**

สารบัญภาพประกอบ

สารบัญภาพประกอบ (ต่อ)

บทที่ ๑
ระบบสารสนเทศและการรักษาความปลอดภัย

การพัฒนาอย่างก้าวกระโดดของเทคโนโลยีสารสนเทศ ทำให้กำลังพลกองทัพอากาศจำเป็นที่จะต้องปรับตัวอย่างรวดเร็ว เพื่อให้ก้าวทันการเปลี่ยนแปลงที่เกิดขึ้น โดยเฉพาะอย่างยิ่งกำลังพลที่ปฏิบัติงานกับระบบสารสนเทศของหน่วยงาน เพื่อก่อให้เกิดความสำเร็จในภารกิจภายใต้การใช้ประโยชน์และการรักษาความปลอดภัยของระบบสารสนเทศอย่างมีประสิทธิภาพและประสิทธิผล

การมองภาพองค์รวมของเทคโนโลยีสารสนเทศและการสื่อสารแบบเชิงระบบ เป็นสิ่งจำเป็นที่ขาดไม่ได้และถือเป็นส่วนหนึ่งขององค์ประกอบสำคัญของกำลังพลที่ปฏิบัติงานกับระบบสารสนเทศ ซึ่งใช้ทั้งศาสตร์ความรู้ทางด้านวิชาการและศิลปะในการเชื่อมโยงความสัมพันธ์ขององค์ประกอบทั้งหมดในระบบสารสนเทศ คุณสมบัติที่พึงประสงค์ของระบบสารสนเทศ ภัยคุกคามกับวัตถุประสงค์และเป้าหมายของภัยคุกคามนั้นๆ ตลอดจนการรักษาความปลอดภัยระบบสารสนเทศ โดยจะต้องสามารถมองภาพความสัมพันธ์ทั้งหมดได้อย่างเข้าใจ เพื่อการใช้เทคโนโลยีสารสนเทศสนับสนุนแผนในการพัฒนาขับเคลื่อนการดำเนินงานของหน่วยงานต่อไปได้อย่างเหมาะสม

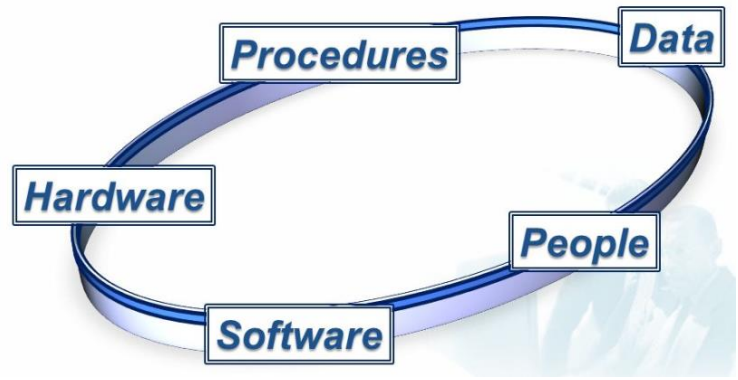
ในการปฏิบัติงานกับระบบสารสนเทศ ซึ่งต้องมีการใช้เทคโนโลยีสารสนเทศและการสื่อสารเป็นองค์ประกอบสำคัญเพื่อให้การดำเนินงานเป็นไปอย่างรวดเร็วและมีประสิทธิภาพนั้น มีความจำเป็นที่จะต้องคำนึงถึงด้านการรักษาความปลอดภัยระบบสารสนเทศของหน่วยงานประกอบไปด้วยเสมอ เนื่องจากการรักษาความปลอดภัยที่ไม่ดีพอ อาจนำมาซึ่งปัญหาและข้อขัดข้องในการดำเนินงานของหน่วยได้ ดังนั้นจึงควรที่จะต้องมีความรู้ความเข้าใจเกี่ยวกับองค์ประกอบที่เกี่ยวข้องกับระบบสารสนเทศ คุณสมบัติด้านความปลอดภัยของระบบสารสนเทศ ภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศและแนวทางในการป้องกัน นอกจากนี้ ยังรวมถึงการคำนึงถึงบทบาทของ Peopleware กับการรักษาความปลอดภัย การกำหนดรหัสผ่านและความปลอดภัย ความรู้ความเข้าใจเกี่ยวกับนำอุปกรณ์ส่วนบุคคลมาบูรณาการใช้ในหน่วยงาน ตลอดจนการใช้บริการจัดเก็บข้อมูลบน Cloud Services กับการรักษาความปลอดภัยด้วย ดังนี้

๑.๑ องค์ประกอบที่เกี่ยวข้องกับระบบสารสนเทศ

“ระบบสารสนเทศ” เป็นระบบที่ประกอบด้วยกลุ่มของส่วนประกอบเชิงสารสนเทศ จำนวน ๕ ส่วน (ภาพที่ ๑) ได้แก่ ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) บุคลากร (People) ข้อมูล (Data) และกระบวนการปฏิบัติ (Procedures) ที่มีการทำงานร่วมกัน เพื่อให้ได้มาซึ่งสารสนเทศ (Information) ที่ใช้ประกอบการตัดสินใจในการบริหารจัดการที่สามารถตอบโจทย์ได้ตรงตามความต้องการของหน่วยงาน

โดย ฮาร์ดแวร์ (Hardware) หมายถึง คอมพิวเตอร์และเครือข่ายตลอดจนอุปกรณ์สื่อสารข้อมูลแบบพกพาและอุปกรณ์ต่อพ่วงอื่นๆ เช่น เครื่องคอมพิวเตอร์แบบตั้งโต๊ะ เครื่องคอมพิวเตอร์แบบโน้ตบุ้ค อุปกรณ์ประเภทสมาร์ทโฟนและแท็บเล็ต อุปกรณ์เครือข่าย เครื่องพิมพ์ โปรเจ็คเตอร์ คีย์บอร์ด เม้าส์ และอุปกรณ์จัดเก็บข้อมูลแบบพกพา (Flash Drive/External Harddisk) เป็นต้น ซอฟต์แวร์ (Software) หมายถึง โปรแกรมระบบปฏิบัติการและโปรแกรมประยุกต์ที่ใช้ในการปฏิบัติงาน เช่น ระบบปฏิบัติการวินโดวส์ และโปรแกรมไมโครซอฟต์ออฟฟิศ เป็นต้น บุคลากร

(People) หมายถึงคนหรือผู้ที่เกี่ยวข้องกับหน่วยงานทุกระดับ ตั้งแต่ ผู้บริหาร ผู้ดูแลระบบ ไปจนถึงผู้ใช้งาน ข้อมูล (Data) หมายถึงข้อมูลดิบและสารสนเทศซึ่งเป็นข้อมูลดิบที่ผ่านการประมวลผลแล้ว และขั้นตอนการปฏิบัติ (Procedures) หมายถึงกระบวนการหรือขั้นตอนการปฏิบัติงานในหน่วยงานที่เกี่ยวข้อง



ภาพที่ ๑.๑ องค์ประกอบของระบบสารสนเทศ

ทั้งนี้ ในส่วนของ ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลนั้น สามารถมองรวมเป็นกลุ่มของ “เทคโนโลยี” ซึ่งประกอบไปด้วย เทคโนโลยีเครือข่ายคอมพิวเตอร์และการสื่อสารโทรคมนาคม (Computer Network and Telecommunication Technology) เทคโนโลยีซอฟต์แวร์ (Software Technology) และเทคโนโลยีฐานข้อมูล (Database Technology) ทำให้เมื่อมีการกล่าวถึงระบบสารสนเทศใดๆ จะสามารถแยกออกเป็น ๓ กลุ่ม (ภาพที่ ๑.๒) ได้แก่ **เทคโนโลยี บุคลากร** และ **กระบวนการ**

ระบบสารสนเทศ				
Hardware	Software	Data	People	Procedures
Computer Network & Telecommunication, Software, Database			People	Procedures
เทคโนโลยี			บุคลากร	กระบวนการ

ภาพที่ ๑.๒ กลุ่มองค์ประกอบของระบบสารสนเทศ

๑.๒ คุณสมบัติด้านความปลอดภัยของระบบสารสนเทศ

จากกลุ่มองค์ประกอบของระบบสารสนเทศ ซึ่งแบ่งออกเป็น เทคโนโลยี บุคลากร และกระบวนการ ทำให้ทราบถึงความสัมพันธ์ในการปฏิบัติงานกับระบบสารสนเทศว่าเป็นการปฏิบัติงาน

ของบุคลากรที่เกี่ยวข้องทุกระดับ ตามกระบวนการขั้นตอนที่กำหนดไว้ โดยใช้เทคโนโลยีสารสนเทศเป็นเครื่องมือในการปฏิบัติงาน เพื่อให้บรรลุวัตถุประสงค์หรือเป้าหมายในการปฏิบัติงาน ทำให้การรักษาความปลอดภัยของระบบสารสนเทศ หมายความถึงการป้องกันความเสียหายอันอาจเกิดขึ้นกับข้อมูลและอุปกรณ์เครือข่ายคอมพิวเตอร์และการสื่อสารที่ใช้งานในหน่วยงาน และการแก้ไขเมื่อเกิดความเสียหายขึ้น

คุณสมบัติด้านความปลอดภัยของระบบสารสนเทศ ประกอบไปด้วย ๕ คุณสมบัติหลัก โดยแบ่งออกเป็น ๒ ด้านที่สำคัญ ได้แก่ คุณสมบัติการรักษาความปลอดภัยด้านเทคโนโลยี (Hardware/Software/Data) และ คุณลักษณะการรักษาความปลอดภัยด้านบุคลากร (People) โดยคุณสมบัติการรักษาความปลอดภัยด้านเทคโนโลยีประกอบไปด้วย ๓ คุณสมบัติ ได้แก่ **การรักษาความลับของข้อมูล** (Data Confidentiality) **การรักษาความถูกต้องของข้อมูล** (Data Integrity) และ **การคงไว้ซึ่งความพร้อมในการใช้งานของระบบ** (System Availability) และคุณลักษณะการรักษาความปลอดภัยด้านบุคลากร ประกอบไปด้วย ๒ คุณสมบัติหลัก ได้แก่ **การรักษาความเป็นส่วนตัวของผู้ใช้งาน** (Privacy) และ**การป้องกันการปฏิเสธความรับผิดชอบ** (Non-Repudiation) ดังนี้

๑.๒.๑ การรักษาความลับของข้อมูล (Data Confidentiality)

หมายถึง การรับประกันถึงความปลอดภัยของข้อมูลในระบบสารสนเทศของหน่วยงานว่าผู้ที่ไม่มีส่วนเกี่ยวข้องหรือไม่มีสิทธิ์จะไม่สามารถเข้าถึงเนื้อหาของข้อมูล (Data Content) ได้

๑.๒.๒ การรักษาความถูกต้องของข้อมูล (Data Integrity)

หมายถึง การยืนยันถึงความถูกต้องครบถ้วนของข้อมูลที่มีการรับส่งในระบบสารสนเทศของหน่วยงานว่าจะไม่ถูกเปลี่ยนแปลง/แก้ไขโดยผู้ไม่ประสงค์ดี และในกรณีที่ข้อมูลถูกเปลี่ยนแปลง/แก้ไข ผู้รับข้อมูลจะทราบได้ว่าข้อมูลนั้นไม่เหมือนกับข้อมูลที่ถูกส่งมาจากต้นทาง

๑.๒.๓ การคงไว้ซึ่งความพร้อมในการใช้งานของระบบ (System Availability)

หมายถึง การรับประกันความพร้อมในการใช้งานอุปกรณ์เครือข่ายคอมพิวเตอร์และการสื่อสารของหน่วยงาน ตลอดจนความพร้อมใช้งานของข้อมูลและบริการประเภทต่างๆ ในระบบสารสนเทศ ทุกครั้งที่ผู้ใช้มีความต้องการใช้งาน

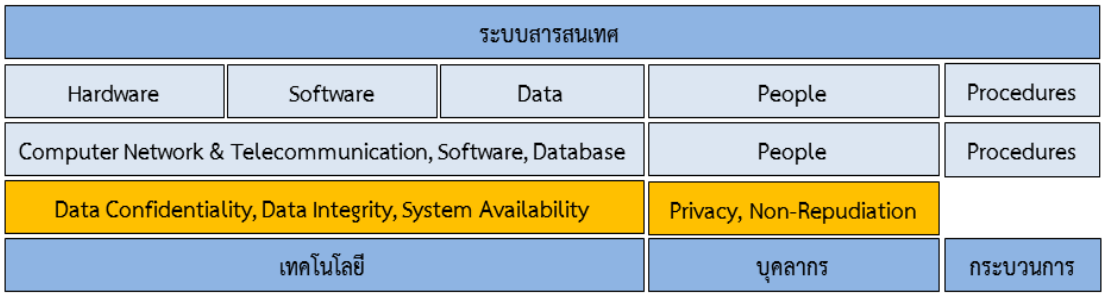
๑.๒.๔ การรักษาความเป็นส่วนตัว (Privacy)

หมายถึง การรับประกันถึงสิทธิในการเข้าถึงและใช้งานทรัพยากรด้านสารสนเทศที่ได้รับการจัดสรรของผู้ใช้งาน ว่าจะไม่ถูกผู้หนึ่งผู้ใดละเมิดสิทธิในการเข้าถึงและใช้งานทรัพยากรนั้นๆ ได้

๑.๒.๕ การป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation)

หมายถึง การยืนยันถึงตัวบุคคลหรือการพิสูจน์ถึงตัวตนของผู้กระทำการใดๆ กับข้อมูลในระบบสารสนเทศเพื่อป้องกันการปฏิเสธความรับผิดชอบในภายหลัง

จะเห็นได้ว่า ๒ คุณสมบัติแรก (Data Confidentiality, Data Integrity, System Availability) นั้นเกี่ยวข้องกับกลุ่มองค์ประกอบด้าน **เทคโนโลยี** และ ๒ คุณสมบัติหลัง (Privacy, Non-Repudiation) นั้นเกี่ยวข้องกับองค์ประกอบด้าน **บุคลากร** ในระบบสารสนเทศของหน่วยงาน (ภาพที่ ๑.๓)



ภาพที่ ๑.๓ คุณสมบัติด้านความปลอดภัยของระบบสารสนเทศ

๑.๓ ภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของหน่วยงานและแนวทางการป้องกัน

ภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของหน่วยงาน มีด้วยกันหลากหลายรูปแบบ ซึ่งแต่ละรูปแบบอาจมีวัตถุประสงค์และเป้าหมายที่แตกต่างกันออกไป อย่างไรก็ตาม ภัยคุกคามทางไซเบอร์นั้น ล้วนแล้วแต่มีวัตถุประสงค์ในการมุ่งทำลาย หรือลดทอนคุณสมบัติด้านความปลอดภัยของระบบสารสนเทศ (Data Confidentiality, Data Integrity, System Availability, Privacy, Non-Repudiation) อย่างใดอย่างหนึ่งหรือหลายอย่างพร้อมกันในเวลาเดียวกันด้วยกันทั้งสิ้น สรุปได้ ดังนี้

๑.๓.๑ ไวรัสคอมพิวเตอร์ (Virus) คือ ชุดคำสั่งหรือโปรแกรมคอมพิวเตอร์ที่เขียนขึ้นมาเพื่อก่อกวนหรือสร้างผลกระทบให้กับการทำงานของเครื่องคอมพิวเตอร์ตลอดจนข้อมูลในเครื่องคอมพิวเตอร์ ทั้งในลักษณะของการทำลายข้อมูลหรือการทำให้ไม่สามารถเรียกใช้ข้อมูลในเวลาที่ต้องการได้ การดักจับข้อมูลสำคัญ และการทำให้เครื่องคอมพิวเตอร์ทำงานไม่ปกติหรือไม่สามารถใช้งานได้ในเวลาที่ต้องการ แบ่งออกเป็นประเภทต่างๆ ได้ดังนี้

❒ บูตเซกเตอร์ไวรัส (Boot Sector Viruses) เป็นไวรัสที่ฝังตัวอยู่ในส่วนของ Master Boot Record ของฮาร์ดดิสก์ ซึ่งเป็นส่วนที่จะเรียกระบบปฏิบัติการ (Operating System) ของคอมพิวเตอร์ขึ้นมาทำงาน ทำให้ทุกครั้งที่บูตเครื่องคอมพิวเตอร์ขึ้นมา ไวรัสจะเริ่มทำงานก่อนและเข้าไปฝังตัวอยู่ในหน่วยความจำเพื่อเตรียมพร้อมที่จะทำงานตามที่ได้ถูกโปรแกรมไว้เหมือนไม่มีอะไรเกิดขึ้น

❒ ไฟล์ไวรัส (File Viruses) เป็นไวรัสที่แฝงตัวอยู่ในรูปของไฟล์ข้อมูล เช่นไฟล์ข้อมูลประเภท .exe .com .dll เป็นต้น ซึ่งเมื่อมีการเรียกไฟล์ที่ติดไวรัสขึ้นมา ส่วนของไวรัสจะฝังตัวเข้าไปอยู่ในหน่วยความจำ โดยเมื่อมีการเรียกโปรแกรมอื่นขึ้นมาทำงานต่อ ไวรัสจะสำเนาตัวเองเข้าไปในโปรแกรมเหล่านั้นแล้วแพร่ระบาดต่อไป

❒ ม้าโทรจัน (Trojan Horses) เป็นไวรัสที่แฝงตัวเข้าไปในระบบคอมพิวเตอร์แล้วทำการดักจับข้อมูลสำคัญต่างๆ เช่น รหัสผ่าน และส่งกลับไปยังผู้ประสงค์ร้ายเพื่อเป็นข้อมูลสำหรับใช้ในการโจมตีตลอดจนติดตามหรือควบคุมการทำงานของเครื่องคอมพิวเตอร์ที่ติดไวรัส

❒ มาโครไวรัส (Macro Viruses) เป็นไวรัสในลักษณะของมาโครหรือชุดคำสั่งที่สามารถทำงานอัตโนมัติเมื่อถูกเรียกใช้ฟังก์ชั่นมาโคร ส่งผลต่อการทำงานของโปรแกรมประยุกต์

ประเภทหน่วยงาน เช่น MS Word, Excel, PowerPoint โดยจะเกิดการหยุดชะงักของการเรียกใช้ไฟล์โดยไม่ทราบสาเหตุ หรือทำให้ไฟล์เสียหาย หรือขัดขวางต่อกระบวนการสั่งพิมพ์ เป็นต้น

❒ หนอนคอมพิวเตอร์ (Worm) เป็นไวรัสประเภทที่สามารถกระจายตัวเองข้ามเครื่องคอมพิวเตอร์ผ่านระบบเครือข่ายไปติดยังเครื่องคอมพิวเตอร์อื่นที่อยู่ในระบบเครือข่ายได้

แนวทางการป้องกันไวรัสคอมพิวเตอร์สามารถปฏิบัติได้ ดังนี้

๑) ติดตั้งซอฟต์แวร์ป้องกันไวรัส และทำการอัพเดทส่วนของ Engine และฐานข้อมูลไวรัส ให้เป็นปัจจุบันเสมอ

๒) อัพเดทระบบปฏิบัติการคอมพิวเตอร์ (Operating System: OS) ให้เป็นปัจจุบันเสมอ

๓) เปิดใช้งานไฟล์วอล (Firewall) ของเครื่องคอมพิวเตอร์

๔) ปรับแต่งการตั้งค่าการทำงานของระบบปฏิบัติการและโปรแกรมประยุกต์ให้มีความปลอดภัย เช่น ปิดการเรียกใช้มาโครของโปรแกรม Microsoft Office ปิดฟังก์ชั่นการเปิดไฟล์แนบในอีเมลแบบอัตโนมัติ และให้แสดงนามสกุลของไฟล์ทั้งหมด เป็นต้น

๕) ปิดการแชร์ไฟล์ผ่านระบบเครือข่าย หรือแชร์ไฟล์ผ่านระบบเครือข่ายโดยตั้งค่ารหัสผ่านเพื่อป้องกัน

๖) ไม่เปิดอีเมล/ไฟล์แนบ/ลิงค์ ที่มาจากแหล่งที่ไม่รู้จัก หรือรู้จักแต่ผิดปกติวิสัย

๗) ไม่เปิด หรือดาวน์โหลดไฟล์ จากเว็บไซต์ที่อันตราย หรือน่าสงสัย หรือไม่น่าเชื่อถือ

๘) ไม่คลิกในหน้าต่างประเภท Pop-up ให้ปิดโดยคลิกตรงเครื่องหมายกากบาทของหน้าต่าง

๙) สำรองข้อมูลลงในอุปกรณ์จัดเก็บข้อมูลภายนอก (External Disk)

๑.๓.๒ สปายแวร์ (Spyware) คือ ชุดคำสั่งหรือโปรแกรมคอมพิวเตอร์ที่ออกแบบและเขียนขึ้นมาเพื่อสังเกตการณ์หรือดักจับข้อมูลในเครื่องคอมพิวเตอร์โดยที่ผู้ใช้ไม่รู้ตัว มักแฝงตัวเข้ามาในเครื่องคอมพิวเตอร์ขณะที่ผู้ใช้งานทำการท่องอินเทอร์เน็ต โดยมีพฤติกรรมในการดักจับข้อมูลการใช้งานหรือสำรวจข้อมูลสถิติการใช้งานในเครื่องคอมพิวเตอร์ โดยส่วนใหญ่มักแฝงตัวเข้ามาเพื่อโฆษณาสินค้า หรือเปลี่ยนแปลงการตั้งค่าของ เว็บบราวเซอร์ (Web Browser) เพื่อให้เชื่อมต่อไปยังเว็บโฆษณาที่ตั้งค่าไว้ แบ่งเป็นประเภทต่างๆ ได้ ดังนี้

❒ แอดแวร์ (Adware) เป็นสปายแวร์ประเภทส่งแบนเนอร์โฆษณาต่างๆ มาที่เครื่องคอมพิวเตอร์ของผู้ใช้งาน ขณะที่มีการใช้งานอินเทอร์เน็ต

❒ Hijacker เป็นสปายแวร์ประเภทที่เปลี่ยนแปลงหน้าเว็บไซต์ที่ตั้งค่าไว้ในเว็บบราวเซอร์ เช่น หน้าเว็บเริ่มต้น (Start Page) และบันทึกหน้าเว็บไซต์ (Bookmark) ให้เป็นเว็บที่ถูกตั้งค่าไว้

❒ BHO (Browser Helper Objects) and Toolbar เป็นสปายแวร์ประเภทที่เพิ่มเติมฟังก์ชั่นหรือเครื่องมือบนเว็บบราวเซอร์ที่เชื่อมต่อไปยังบริการที่ถูกตั้งค่าไว้

❒ คีย์ล็อกเกอร์ (Keylogger) เป็นสปายแวร์ประเภทที่ดักจับข้อมูลที่มีการพิมพ์ผ่านคีย์บอร์ดของผู้ใช้งาน เพื่อดักจับข้อมูลสำคัญ เช่น รหัสผ่าน หมายเลขบัตรเครดิต เป็นต้น โดยพบว่ามีทั้งแบบซอฟต์แวร์และแบบฝังตัวมากับฮาร์ดแวร์ เช่น ฝังตัวมากับคีย์บอร์ด (Keyboard)

แนวทางการป้องกันสปายแวร์สามารถปฏิบัติได้ ดังนี้

๑) ไม่เปิดอีเมล/ไฟล์แนบ ที่มาจากแหล่งที่ไม่รู้จัก หรือรู้จักแต่ผิดปกติวิสัย

๒) ไม่เปิด หรือดาวน์โหลดไฟล์ จากเว็บไซต์ที่อันตราย หรือน่าสงสัย หรือไม่น่าเชื่อถือ

๓) ไม่คลิกในหน้าต่างประเภท Pop-up ให้ปิดโดยคลิกตรงเครื่องหมายกากบาทของหน้าต่าง

๑.๓.๓ สแปม (Spam) เป็นข้อมูลประเภทการโฆษณาเสนอขายสินค้าหรือบริการออนไลน์ที่ส่งตรงมายังผู้รับซึ่งไม่มีความต้องการและไม่มีเจตจำนงค์ในการรับข้อมูล และส่งมาครั้งละมากๆ หรือส่งมาบ่อยครั้ง สร้างความรำคาญให้แก่ผู้รับและมีผลทำให้พื้นที่การใช้งานทรัพยากรสารสนเทศของผู้ใช้ลดน้อยลง มักส่งมาถึงผู้รับในรูปของไปรษณีย์อิเล็กทรอนิกส์ที่เรียกว่าเมลขยะ (Spam Mail)

แนวทางการป้องกันสแปมสามารถปฏิบัติได้ ดังนี้

๑) พิจารณาให้ดีก่อนสมัครรับบริการหรือข่าวสารใดๆ ทางอินเทอร์เน็ต

๒) ไม่เปิดเผยอีเมลแอดเดรสหรือชื่อบัญชีผู้ใช้งานอื่นสู่สาธารณะโดยไม่จำเป็น

๓) ตั้งค่าการกรองสแปมในอีเมล

๔) แจ้งผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) เพื่อปิดกั้นสแปม

๕) ยกเลิกการรับบริการข่าวสารจากอินเทอร์เน็ตกับผู้ให้บริการ

๑.๓.๔ สนิฟเฟอร์ (Sniffer) คือโปรแกรมประสงค์ร้ายที่แทรกตัวอยู่ในระบบเครือข่ายคอมพิวเตอร์ และคอยดักจับข้อมูลที่วิ่งในระบบเครือข่ายที่มีการใช้งานร่วมกันในหน่วยงาน เพื่อการดักจับข้อมูลสำคัญ เช่น รหัสผ่าน เป็นต้น โดย Sniffer นั้นสามารถปฏิบัติการได้ทั้งแบบในเครือข่ายใช้สายและเครือข่ายไร้สาย (ภาพที่ ๑.๔)

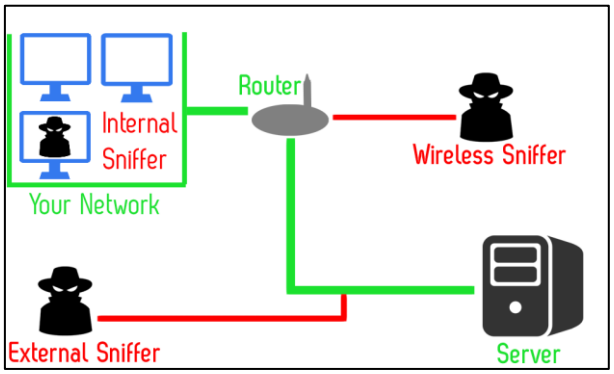
แนวทางการป้องกันสนิฟเฟอร์สามารถปฏิบัติได้ ดังนี้

๑) ใช้อุปกรณ์ Switch แทนอุปกรณ์ Hub

๒) เข้ารหัสข้อมูล/เมล สำคัญที่รับส่ง (Data Encryption, PGP, S/MIME)

๓) เลือกใช้บริการเว็บที่มีการเข้ารหัสข้อมูลด้วย SSL

๔) เชื่อมต่อเข้าระบบเครือข่ายภายในของหน่วยงานด้วยระบบ VPN (Virtual Private Network)



ภาพที่ ๑.๔ สนิฟเฟอร์ (Sniffer) ที่คอยดักจับข้อมูลในระบบเครือข่าย

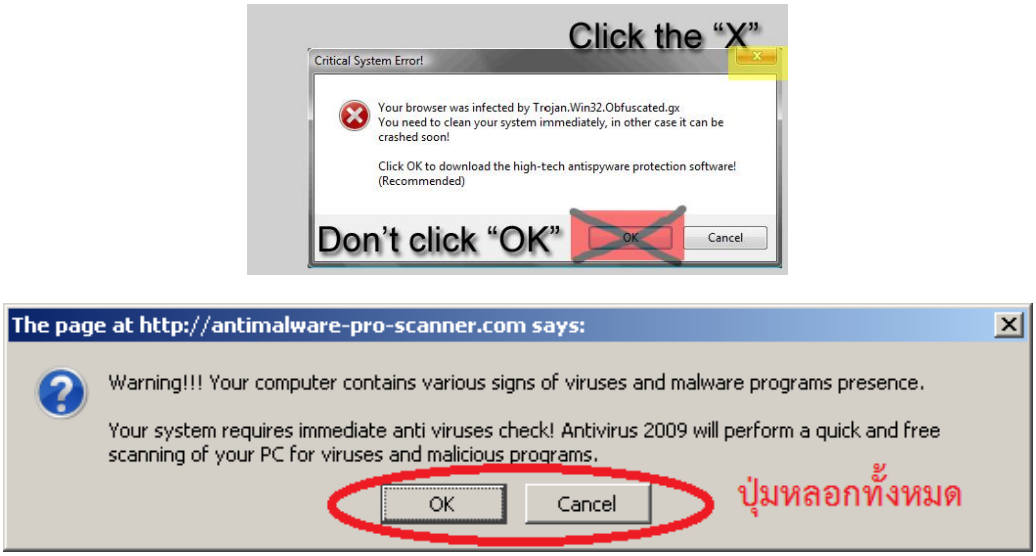
๑.๓.๕ การเข้ารหัสไฟล์เพื่อเรียกค่าไถ่ (Ransomware) คือโปรแกรมประสงค์ร้ายที่จะทำการเข้ารหัสไฟล์ข้อมูลสำคัญในเครื่องคอมพิวเตอร์เพื่อเรียกค่าไถ่ในการถอดรหัสไฟล์กลับคืน เป็นลักษณะของการจับ “ไฟล์สำคัญ” ในคอมพิวเตอร์ของผู้ใช้เป็นตัวประกัน โดยหากผู้ใช้คอมพิวเตอร์ที่เป็นเจ้าของไฟล์สำคัญในเครื่อง ไม่ยอมจ่ายเงินเพื่อเป็นค่าไถ่ ผู้ใช้งานนั้นก็จะไม่สามารถเรียกใช้ไฟล์สำคัญเหล่านั้นได้ ถือเป็นอาชญากรรมทางไซเบอร์รูปแบบหนึ่ง

ตัวอย่างที่พบได้แก่ TROJ_RANSOM.QOWA ในปี 2011, REVETON ในปี ค.ศ. ๒๐๑๒, CryptoLocker ในปี ค.ศ.๒๐๑๓ และ CryptoLocker.F & Cryptowall ในปี ค.ศ.๒๐๑๔ โดยทุกชนิดจะมีรูปแบบและวัตถุประสงค์ในลักษณะเดียวกันคือ ทำให้ไฟล์สำคัญของผู้ใช้งานที่อยู่ในเครื่องคอมพิวเตอร์และในอุปกรณ์สำรองข้อมูลแบบพกพา (Flash Drive, External Harddisk) ที่เชื่อมต่อกับคอมพิวเตอร์อยู่ในขณะนั้นไม่สามารถเปิดใช้ได้ หรือทำให้ผู้ใช้ไม่สามารถเปิดใช้งานเครื่องคอมพิวเตอร์ได้ (ล็อคเครื่องไว้และอาจมีการหลอกแจ้งผู้ใช้งานว่าได้กระทำผิดว่าด้วยการใช้งานคอมพิวเตอร์ในลักษณะที่ไม่เหมาะสม ในรูปของคำแจ้งเตือนจาก FBI เป็นต้น) แล้วทำการเรียกเงินจากผู้ใช้ เพื่อเป็นค่าไถ่ให้กับวิธีการปลดล็อคไฟล์หรือวิธีปลดล็อคเครื่อง ให้สามารถกลับมาใช้งานได้ดังเดิม (ภาพที่ ๑.๕) ซึ่งในปัจจุบันนั้น พบว่ามีการนำรูปแบบของการเข้ารหัสชนิดที่มีความแข็งแกร่งสูง เช่น RSA-2048 Encryption มาใช้ในการล็อค ทำให้ไม่สามารถที่จะทำการปลดล็อคได้โดยง่าย หรือไม่สามารถปลดล็อคได้เลยในทางปฏิบัติ นอกจากจะต้องยอมจ่ายเงินค่าไถ่ เพื่อแลกกับกุญแจสำหรับปลดล็อค หรือไม่ก็ต้องทำการฟอร์แมตเครื่องคอมพิวเตอร์ใหม่

ภาพที่ ๑.๕ ตัวอย่างหน้าจอแสดงการติด Ransomware

Ransomware เป็นโปรแกรมในรูปของ Execute File (.exe) ที่เป็นไฟล์สำหรับใช้ติดตั้งโปรแกรม ซึ่งโดยปกติทั่วไปแล้วจะไม่สามารถแพร่เข้าสู่เครื่องคอมพิวเตอร์ได้แบบอัตโนมัติ เพราะจะถูกปิดกั้นโดยโปรแกรมป้องกันไวรัสในขั้นแรก กล่าวคือจะต้องมีขั้นตอนการดับเบิลคลิกไปที่ตัวไฟล์ .exe ก่อนที่จะเริ่มติดตั้งเสมอ ดังนั้นการติด Ransomware มักจะมาจากการนำโปรแกรม .exe เข้ามาในเครื่องโดยตัวผู้ใช้งานเองโดยไม่รู้ตัวหรือรู้เท่าไม่ถึงการณ์

ช่องทางที่สามารถหลอกผู้ใช้งานให้ดาวน์โหลดโปรแกรมมาลงในเครื่องได้ก็คือ การแฝงตัวมาในรูปของลิงค์ดาวน์โหลดต่างๆ บนเว็บไซต์ในอินเทอร์เน็ต ที่มักจะมีการ Pop-up ขึ้นมาจูงใจและหลอกล่อให้กด (เพื่อดาวน์โหลดและเปิดโปรแกรม) ด้วยการใช้บทโฆษณาจูงใจแบบต่างๆ เช่น “ข้อเสนอพิเศษ” หรือ “คุณเป็นผู้โชคดี” ฯลฯ และในหลายครั้งที่ถูกออกแบบมาให้เริ่มดาวน์โหลดและเปิดโปรแกรมแม้จะกดไปที่ “ปิดหน้าต่าง” หรือ “OK” หรือแม้แต่กดไปที่ “Cancel” ก็ตาม (ปุ่มหลอก) (ภาพที่ ๑.๖)



ภาพที่ ๑.๖ ตัวอย่างปุ่มหลอก

นอกจากนี้ ยังมักพบในรูปแบบของไฟล์แนบที่มาพร้อมกับอีเมล โดยพบมากในรูปแบบของไฟล์บีบอัด (Zip File) ซึ่งผู้รับจะไม่ทราบว่าเมื่อแตกไฟล์ออกมาแล้วจะเป็นไฟล์อะไร หรือในบางกรณีที่เครื่องคอมพิวเตอร์ไม่มีระบบตรวจสแกนไฟล์แนบของอีเมลแบบอัตโนมัติ การแนบไฟล์ที่มีนามสกุลหลอก อาทิเช่น ไฟล์แนบที่มองเห็นเป็นไฟล์เวิร์ด (.docx) หรือไฟล์ PDF (.pdf) แต่จริงๆ แล้วเป็น Execute File (.exe) ทำให้มีผู้คนจำนวนไม่น้อยที่ตกเป็นเหยื่อของอาชญากรรมประเภทนี้แบบไม่ทันรู้ตัว (ภาพที่ ๑.๗)

แนวทางการป้องกันสนิฟเฟอร์สามารถปฏิบัติได้ ดังนี้

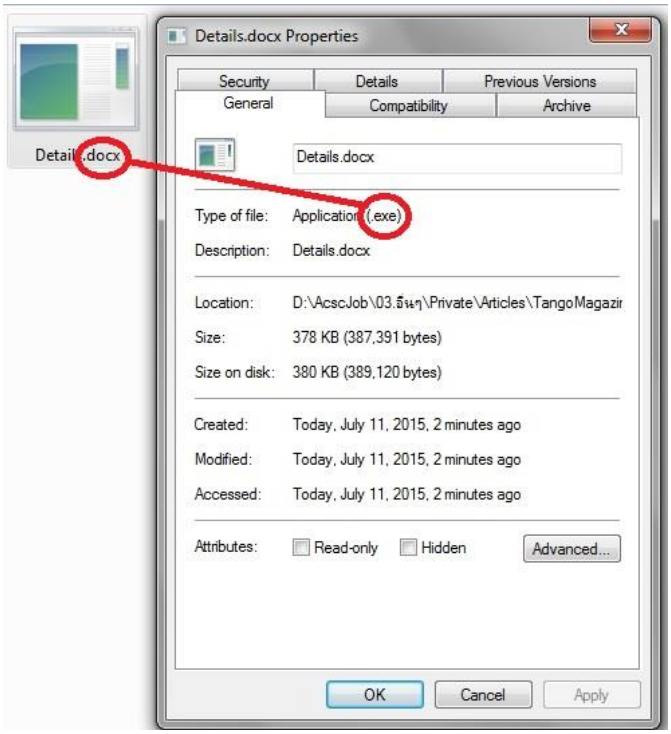
๑) ไม่เปิดเว็บไซต์ประเภทลามกอนาจาร

๒) ไม่เปิดเว็บไซต์และดาวน์โหลดโปรแกรมประเภทผิดกฎหมาย

๓) ไม่เปิดอีเมล/ไฟล์แนบ/ลิงค์ ที่มาจากแหล่งที่ไม่รู้จัก หรือรู้จักแต่ผิดปกติวิสัย

๔) ไม่คลิกในหน้าต่างประเภท Pop-up ให้ปิดโดยคลิกตรงเครื่องหมายกากบาทของหน้าต่าง หรือปิดจาก Task Manager

๕) สำรองข้อมูลลงในอุปกรณ์จัดเก็บข้อมูลภายนอก (External Disk) และถอดการเชื่อมต่อทันทีเมื่ออัพเดทข้อมูลเสร็จ



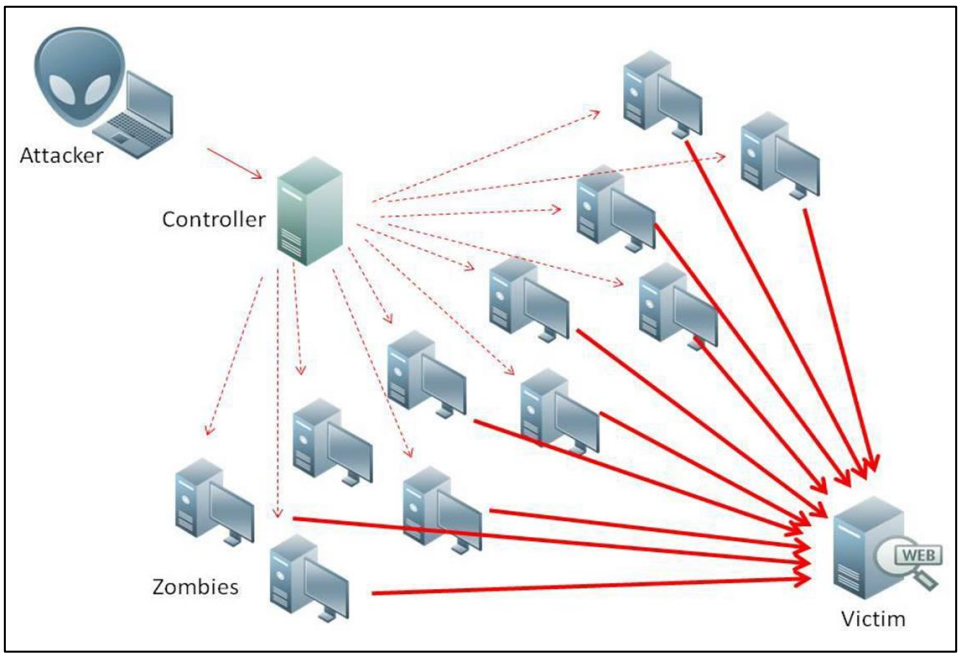
ภาพที่ ๑.๗ ตัวอย่างไฟล์ที่มีนามสกุลหลอก

๑.๓.๖ การระดมโจมตีเพื่อทำให้เครื่องแม่ข่ายไม่สามารถให้บริการได้ (Distributed Denial of Service: DDoS Attack) หมายถึงการระดมโจมตีเครื่องแม่ข่ายเป้าหมายพร้อมกันจากหลายแหล่งที่กระจายตัวอยู่ตามที่ต่างๆ เพื่อให้เกินข้อจำกัดของเครือข่าย ทำให้ระบบการให้บริการของเครื่องเป้าหมายไม่สามารถดำเนินการได้ตามปกติ นับเป็นรูปแบบหนึ่งของการโจมตีทางไซเบอร์ที่มีอานุภาพในการสร้างความเสียหายด้านความพร้อมใช้งานของระบบ (System Availability) ได้ในระดับที่รุนแรง

ตัวอย่างข้อจำกัดของการให้บริการของเครื่องแม่ข่าย เช่น ในขณะที่เรากำลังเรียกเปิดดูเว็บไซต์ใดเว็บไซต์หนึ่งจากเครื่องคอมพิวเตอร์ที่ต่อเชื่อมอินเทอร์เน็ตอยู่ที่บ้าน ในเวลาเดียวกันก็มีผู้ที่กำลังจะเรียกเปิดดูเว็บไซต์เดียวกับเราอีกเป็นจำนวนมหาศาลจากทั่วทุกมุมโลก เครื่องแม่ข่ายของเว็บไซต์ดังกล่าว จะได้รับการร้องขอการต่อเชื่อมกับเครื่องแม่ข่ายที่ให้บริการเว็บ (Web Server) เป็นจำนวนมหาศาลเช่นเดียวกัน ทำให้ทรัพยากรของเครื่องแม่ข่ายถูกใช้เกินกว่าขีดความสามารถที่จะให้บริการได้ ส่งผลให้เครื่องแม่ข่ายเกิดการล่มไม่สามารถให้บริการต่อได้ ก่อให้เกิดความเสียหายต่อการดำเนินการ และยิ่งระบบการให้บริการเกิดการล่มเป็นเวลานานเท่าใด ความเสียหายทางธุรกิจหรือการให้บริการก็ยิ่งมีโอกาสเกิดขึ้นมากเท่านั้น แต่ในความเป็นจริงแล้ว โอกาสที่จะเกิดเหตุการณ์ในลักษณะดังกล่าวจากผู้ใช้งานปกตินั้นเกิดขึ้นได้ยากมาก เพราะขีดความสามารถในการให้บริการของเครื่องแม่ข่ายย่อมมีประสิทธิภาพตลอดจนมี Topology ที่ดีเพียงพอที่จะรองรับการขอใช้บริการจากผู้ใช้งานปกติได้

จากหลักการการของข้อจำกัดในการให้บริการของเครื่องแม่ข่ายนี้ ทำให้เกิดแนวความคิดในการโจมตีทางไซเบอร์จากผู้ไม่ประสงค์ดี ด้วยการ **สร้างกลุ่มของผู้เรียกใช้งานที่มี**

จำนวนมหาศาลขึ้น ทั้งจากการจำลองกลุ่มผู้ใช้งานขึ้นเองด้วยโปรแกรมคอมพิวเตอร์ การระดมพลผู้มีแนวความคิดแบบเดียวกัน หรือการใช้ประโยชน์จากเครื่องคอมพิวเตอร์ อุปกรณ์ Smart Devices และอุปกรณ์เชื่อมต่ออื่นๆในรูปแบบของ IoT (Internet of Things) ด้วยการฝังมัลแวร์ลงในอุปกรณ์นั้นๆ เพื่อประโยชน์ในการควบคุม (Control) การใช้งานจากระยะไกลในรูปแบบของ Zombies/Bots และใช้ปริมาณอันมหาศาลนี้โจมตี (ร้องขอการให้บริการพร้อมๆ กัน) ไปยังเป้าหมายเสมือนหนึ่งว่ามีปริมาณความต้องการเรียกใช้งานเครื่องแม่ข่ายเป้าหมายจริงๆ จากผู้ใช้งาน เพื่อวัตถุประสงค์ในการทำให้เครื่องแม่ข่ายนั้นหยุดการทำงานหรือปิดการให้บริการลง (ภาพที่ ๑.๘)



ภาพที่ ๑.๘ ตัวอย่างลักษณะการโจมตีแบบ DDoS

รูปแบบการโจมตีของ DDoS แบ่งได้เป็น ๒ ลักษณะ ได้แก่ การโจมตีแบบเชิงปริมาณ (Volumetric Attack) และการโจมตีแบบมุ่งเป้าแอพพลิเคชั่นที่ใช้งาน (Application-level Attack) ดังนี้

๑.๓.๖.๑ การโจมตีแบบเชิงปริมาณ (Volumetric Attack) เป็นลักษณะการโจมตีที่มุ่งเป้าทำให้เกิดปริมาณ Traffic เต็ม Bandwidth ของฝั่งผู้ให้บริการ หรือการเรียกใช้ทรัพยากรของเครื่องเป้าหมาย (เช่น หน่วยความจำ, CPU) เกินกว่าที่จะรับได้ เช่น ระดมส่ง UDP Flood (เช่น DNS, SNMP) หรือ ICMP Flood (เช่น Ping) ขนาดแพ็กเก็ตใหญ่ หรือ Open Request จากหลายที่ไปพร้อมๆ กัน ส่งผลให้คิวการให้บริการของเครื่องเป้าหมายเต็มและไม่สามารถให้บริการต่อผู้ใช้งานอื่นๆ ตามปกติได้ นอกจากนี้ยังมีรูปแบบของการเปลี่ยนแปลงค่า Offset ในแพ็กเก็ตข้อมูลกรณีที่แพ็กเก็ตมีขนาดใหญ่ ต้องแบ่งย่อยออกเป็น Fragment เล็กๆหลายส่วน เพื่อไปประกอบร่างกันเป็นแพ็กเก็ตใหญ่ที่ปลายทาง ที่เรียกว่าแบบ Teardrop ซึ่งผู้โจมตีจะเปลี่ยนค่า Offset ในแพ็กเก็ตส่วนกลางๆ

ทำให้เครื่องรับปลายทางเกิดความสับสนเวลาที่จะเรียงแพ็กเก็ตย่อยกลับคืน โดยหากระบบปลายทางไม่สามารถรับมือกับปัญหานี้ได้ ก็จะทำให้ระบบหยุดการทำงานได้ สำหรับความรุนแรงของการโจมตีจะวัดเป็น **Bits** per Second (bps) หรือ **Packets** per Second (pps)

๑.๓.๖.๒ การโจมตีแบบมุ่งเป้าแอพพลิเคชั่นที่ใช้งาน (Application-level Attack) เป็นลักษณะการโจมตีที่ผู้ไม่ประสงค์ดีจะระดมส่ง Request การร้องขอใช้งานแอพพลิเคชั่น (โจมตีโดยใช้ Bandwidth น้อย แต่ส่งติดต่อกันต่อเนื่อง) โดยเฉพาะบริการเว็บไซต์ (Web Service) ซึ่งได้แก่การส่ง HTTP Request ติดต่อกันไปยัง Web Server เพื่อทำให้เครื่องล่ม เช่น ปรากฏการณ์การเปิดเว็บไซต์ของกลุ่มคนจำนวนมาก แล้วพร้อมใจกันกด F5 เพื่อ Refresh หน้าเว็บเพจใหม่ (คือการส่ง HTTP Request ไปใหม่เรื่อยๆ ติดต่อกัน) สำหรับความรุนแรงของการโจมตีจะวัดเป็น **Requests** per Second (rps)

ปัจจุบันพบว่ามีรูปแบบใหม่ของการโจมตีของ DDoS ในลักษณะของการส่ง Request ไปยัง DNS Server (Domain Name System Server) เพื่อร้องขอข้อมูล IP Address จากชื่อ Web ที่สอบถามไป แต่ไม่ใช่การร้องขอข้อมูลแบบปกติที่แฝงไว้ซึ่ง Request ที่ก่อให้เกิด Response ขนาดใหญ่จำนวนมหาศาล โดยให้ส่งข้อมูล Response ทั้งหมดกลับไปที่เครื่องเป้าหมายเพียงเครื่องเดียวแทน หลักการคือใช้วิธีการปลอมแปลง IP Address ต้นทางให้เป็น IP Address ของเครื่องเป้าหมายแล้วส่ง DNS Request ไปยัง DNS Server ที่อนุญาตให้มีการทำ Recursion หรือการสอบถามเพื่อขอข้อมูล IP Address จากชื่อ Web ต่อไปยัง DNS อื่น (Open DNS Resolver) และให้ตอบกลับไปที่ IP Address ของเครื่องเป้าหมายตามที่ระบุไว้ โดยหากใช้งานร่วมกับอุปกรณ์ที่เป็น Zombies/Botnets จำนวนมากในการส่ง DNS Request ด้วยแล้ว DNS Response ขนาดใหญ่จำนวนมหาศาลจะถูกส่งกลับไปยังเครื่องเป้าหมายที่ระบุไว้เพียงเครื่องเดียว ซึ่งผลที่ตามมาก็คือ ทำให้ Bandwidth ปลายทางเต็ม การประมวลผลการทำงานไม่ทัน และสุดท้ายไม่สามารถให้บริการต่อได้ การโจมตีในลักษณะนี้เรียกว่า **DNS DDoS Amplification**

นอกเหนือจากการใช้ประโยชน์จาก DNS Server แล้ว ยังมีการใช้ประโยชน์จาก NTP Server (Network Time Server) ในลักษณะที่คล้ายกันอีกด้วย เช่น ส่ง “get monlist” Request ไปยัง NTP Server โดย NTP Server จะส่งข้อมูลของเครื่องจำนวน ๖๐๐ เครื่องล่าสุด (ทั้งเครื่อง Client ทั่วไปและเครื่อง Server อื่นที่ติดต่อเข้ามา) ที่ติดต่อกับ NTP Server กลับไป ซึ่งข้อมูลตอบกลับนับว่าเป็นข้อมูลที่มีขนาดใหญ่ และเช่นเดียวกัน หากใช้งานร่วมกับอุปกรณ์ที่เป็น Zombies/Botnets จำนวนมากในการส่ง Request ด้วยแล้ว Response ขนาดใหญ่จำนวนมหาศาลจะถูกส่งกลับไปยังเครื่องเป้าหมายที่ระบุไว้เพียงเครื่องเดียว ส่งผลทำให้ระบบล่มและหยุดการให้บริการ การโจมตีในลักษณะนี้เรียกว่า **NTP DDoS Amplification**

เทคนิคในการยืมมือ Zombies/Botnet ในการร่วมระดมส่ง Request จำนวนมากไปยังเครื่อง Server ที่ให้บริการตามปกติ โดยปลอมแปลง IP Address ต้นทางให้เป็น IP Address ของเครื่องเป้าหมาย เพื่อให้เครื่อง Server ส่ง Response ที่มีขนาดใหญ่กลับไปยังเครื่องเป้าหมายที่ระบุไว้เพียงเครื่องเดียว นับเป็นวิธีที่มีประสิทธิภาพและป้องกันได้ยาก เนื่องจากข้อมูล Response ถือเป็นข้อมูลถูกต้องตามรูปแบบ (Legitimate Data) จากเครื่อง Server ที่มีตัวตนเชื่อถือได้ (Valid Server)

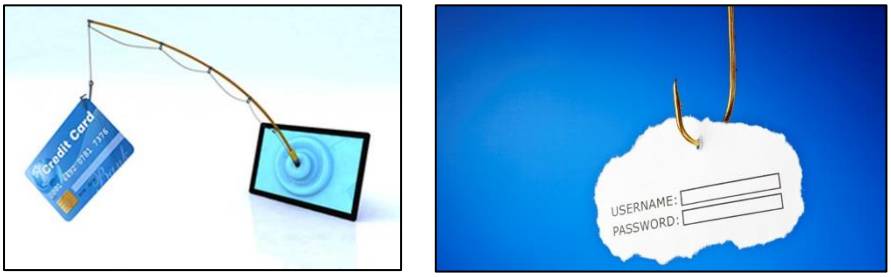
แนวทางการป้องกันการระดมโจมตีเพื่อทำให้เครื่องแม่ข่ายไม่สามารถให้บริการได้ (DDoS) สามารถปฏิบัติได้ ดังนี้

๑) ติดตั้งระบบป้องกันการโจมตีแบบ DDoS โดยเฉพาะ
๒) ตั้งค่าการกรองแพ็กเก็ตบนไฟร์วอลและเราท์เตอร์
๓) นำเทคนิค Anycast มาใช้ในการบริหารจัดการ Traffic ในเครือข่าย
๔) ติดตั้งซอฟต์แวร์เฉพาะเพิ่มเติม เช่น TCP Sync Flooding
๕) ปิดพอร์ตที่ไม่มีการใช้งานบน Web Server
๖) เก็บสถิติและตรวจตราปริมาณ Traffic ในเครือข่ายเพื่อการเฝ้าระวังอยู่เสมอ
๗) เตรียมระบบเครือข่ายสำรอง เพื่อให้บริการแทน กรณีเครือข่ายหลักไม่สามารถให้บริการได้

๑.๓.๗ การหลอกลวง (Phishing) เป็นวิธีการหรือกระบวนการในการหลอกลวงบุคคลเพื่อให้ได้มาซึ่งข้อมูลสำคัญ เช่น ชื่อบัญชีผู้ใช้งาน รหัสผ่าน และหมายเลขบัตรเครดิต ฯลฯ เพื่อวัตถุประสงค์ในการนำไปแสวงหาผลประโยชน์ในรูปแบบใดรูปแบบหนึ่ง (ภาพที่ ๑.๙) ซึ่งในโลกออนไลน์นั้น สิ่งสำคัญในการบ่งบอกตัวตน (Identity) ได้แก่ ชื่อบัญชีผู้ใช้งาน (User Account Name) ของการให้บริการประเภทต่างๆ เช่น ชื่อบัญชีอีเมล ชื่อบัญชี Facebook ชื่อบัญชีธนาคารอิเล็กทรอนิกส์ (e-Banking) นอกจากนี้ ในการพิสูจน์เพื่อยืนยันตัวตนของผู้ใช้งานส่วนใหญ่ก็มักใช้รหัสผ่าน (Password) เฉพาะของแต่ละบัญชีที่ผู้ใช้งานเป็นผู้ตั้งขึ้น เป็นตัวยืนยันตัวตนที่แท้จริงของผู้ใช้งาน และในการทำธุรกรรมที่เกี่ยวข้องกับการเงิน จะมีเรื่องของหมายเลขบัตรเครดิต วันหมดอายุของบัตร วงเงินในบัตร หรือหมายเลขด้านหลังบัตรเครดิต เข้ามาเป็นปัจจัยสำคัญด้วยเสมอ

ปัจจุบัน มีคนจำนวนมากที่ใช้งานบริการต่างๆ ในโลกออนไลน์ และการใช้บริการนั้นก็สามารถกระทำได้ทันทีหากป้อนค่าชื่อบัญชีผู้ใช้และรหัสผ่านได้อย่างถูกต้อง เช่นเดียวกัน การสั่งซื้อสินค้าออนไลน์ก็สามารถกระทำได้ทันทีหากป้อนค่าเกี่ยวกับบัตรเครดิตได้ถูกต้อง ทำให้ข้อมูลเกี่ยวกับชื่อบัญชีผู้ใช้งาน รหัสผ่าน และบัตรเครดิต เป็นสิ่งที่มีความสำคัญอย่างยิ่ง

จากการที่การเข้าใช้งานบริการต่างๆ นั้นสามารถกระทำได้โดยง่ายผ่านชื่อบัญชีผู้ใช้งานและรหัสผ่าน (และข้อมูลบัตรเครดิตกรณีมีการชำระค่าสินค้าหรือบริการ) ทำให้เกิดมีกลุ่มของผู้ไม่ประสงค์ดีที่แสวงหาประโยชน์จากผู้อื่นด้วยการขโมยข้อมูลสำคัญดังกล่าวไป แล้วนำไปใช้ในทางที่ไม่เหมาะสมแต่สามารถสร้างประโยชน์บางอย่างให้กับตัวเองได้ จึงเกิดมีพฤติกรรมของการพยายามให้ได้มาซึ่งข้อมูลดังกล่าวขึ้นในหลากหลายรูปแบบ



ภาพที่ ๑.๙ Phishing การหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลสำคัญ

หากเป็นชื่อบัญชีผู้ใช้และรหัสผ่านที่ใช้กับบริการของธนาคารแบบออนไลน์ กระบวนการยับยั้งหรือยกเลิกธุรกรรมนั้นๆ อาจกระทำไม่ทัน และถึงแม้ว่าจะสามารถพิสูจน์ทราบในภายหลังได้ว่า ผู้ใช้บริการไม่ได้เป็นผู้กระทำธุรกรรม แต่ในเงื่อนไขของการรับบริการแบบออนไลน์ต่างๆ ก็มักจะมีระบุไว้อย่างชัดเจนว่าผู้ให้บริการจะไม่รับผิดชอบต่อความเสียหายใดๆ ในกรณีที่เกิดจากการรั่วไหลของข้อมูลที่ไม่ได้มาจากความผิดพลาดของผู้ให้บริการ (ภาพที่ ๑.๑๐)

2. การกระทำใด ๆ ที่กระทำผ่านบริการทางอิเล็กทรอนิกส์ของธนาคารแห่งประเทศไทย หรือการนำข้อมูลใด ๆ ที่ได้จากบริการทางอิเล็กทรอนิกส์ของธนาคารแห่งประเทศไทย โดยใช้ชื่อผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ของผู้ใช้บริการ ไม่ว่าการกระทำนั้นจะเกิดขึ้นโดยผู้ใช้บริการหรือบุคคลอื่นใด ผู้ใช้บริการตกลงให้ถือว่าเป็นการกระทำที่ถูกต้องสมบูรณ์ของผู้ใช้บริการ และผู้ใช้บริการยินยอมรับผิดชอบในการกระทำดังกล่าวเสมือนว่าผู้ใช้บริการเป็นผู้กระทำด้วยตนเอง

3. ผู้ใช้บริการตกลงว่าธนาคารแห่งประเทศไทยไม่ต้องรับผิดชอบในความเสียหายใด ๆ ที่เกิดขึ้นหรืออาจเกิดขึ้นกับผู้ใช้บริการ หรือบุคคลภายนอกจากการเข้าใช้บริการทางอิเล็กทรอนิกส์ของธนาคารแห่งประเทศไทย ไม่ว่าโดยเหตุประการใด

ภาพที่ ๑.๑๐ ตัวอย่างข้อความแสดงข้อตกลงในการใช้บริการทางอิเล็กทรอนิกส์ของธนาคาร

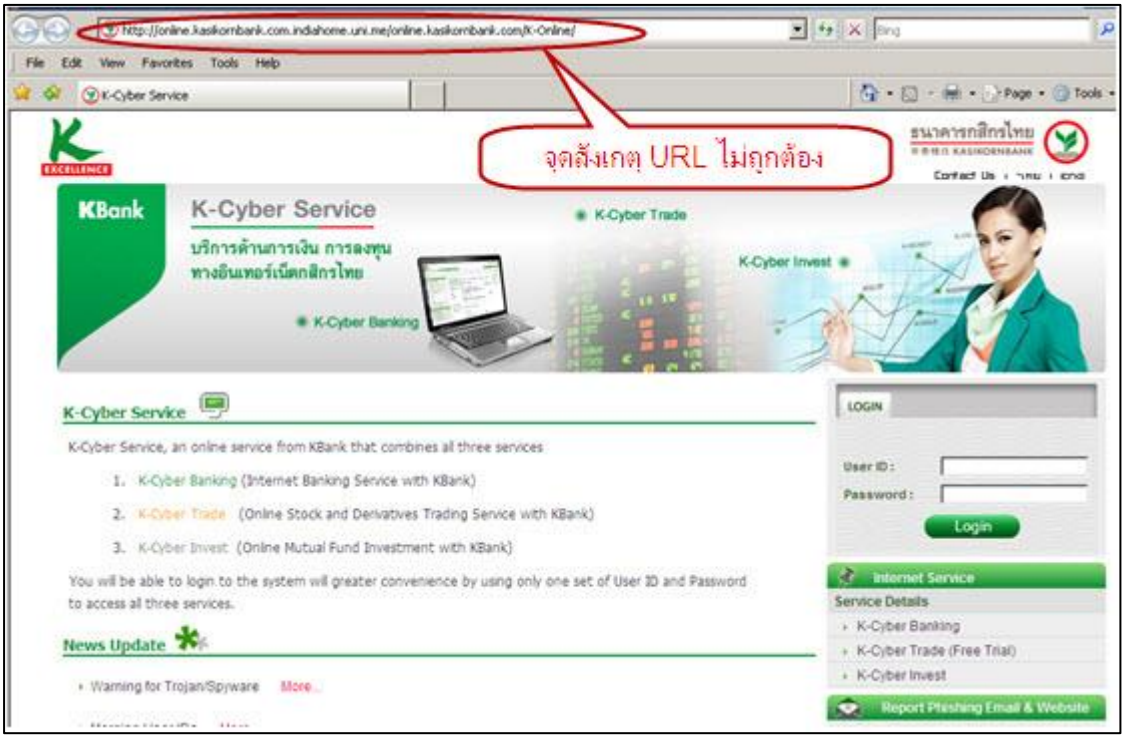
ประเด็นต่อมา หากเป็นชื่อบัญชีผู้ใช้และรหัสผ่านของบัญชีอีเมล Facebook, LINE หรือบริการทางด้านการติดต่อสื่อสารอื่นๆ ผู้ไม่ประสงค์ดีก็สามารถที่จะเข้าไปดูข้อมูลทั้งหมดที่อยู่ภายในบริการที่เป็นของผู้รับบริการได้ เช่น เรียกดูอีเมล เรียกดูข้อมูลประวัติผู้ใช้งาน เรียกดูประวัติการโพสต์ ประวัติการการแชท ฯลฯ ได้ ทำให้สามารถที่จะได้มาซึ่งข้อมูลสำคัญเพิ่มขึ้น เช่น ประวัติการจับจ่ายใช้สอย ประวัติการเดินทาง ประวัติการพบปะสนทนา และที่สำคัญคือสามารถที่จะได้มาซึ่งข้อมูลของคู่สนทนาหรือของกลุ่มสนทนาของเจ้าของบัญชีผู้ใช้งานนั้นได้อีกด้วย โดยในหลายกรณี ผู้ไม่ประสงค์ดีจะล็อคอินเข้าใช้งานและปลอมตัวเป็นเจ้าของตัวจริง แล้วส่งเมลหรือข้อความสนทนาไปยังเพื่อนหรือกลุ่มเพื่อน เพื่อสร้างเรื่องว่าตนเองมีความลำบากต้องใช้เงินและหลอกให้โอนเงินให้ เป็นต้น ซึ่งภาพข่าวทางสื่อต่างๆ ก็พิสูจน์อย่างชัดเจนว่า มีผู้หลงเชื่อแล้วโอนเงินหรือให้ความช่วยเหลือในรูปแบบต่างๆ อยู่เสมอ เนื่องจากคิดว่าเป็นเพื่อนของตนเองและกำลังมีความเดือดร้อนจริง

นอกจากนี้ จุดอ่อนหนึ่งที่สำคัญของผู้ใช้บริการออนไลน์โดยทั่วไปก็คือ มักจะใช้รหัสผ่านตัวเดียวกันกับบัญชีผู้ใช้บริการประเภทอื่นด้วย (ไม่อยากจำรหัสผ่านหลายตัว) ทำให้ การได้มาซึ่งชื่อบัญชีและรหัสผ่านผู้ใช้งานเพียงอันเดียว สามารถต่อยอดได้อย่างมีประสิทธิภาพในอีกหลายบริการที่ผู้ใช้บริการตัวจริงใช้บริการ ในบางกรณีที่ผู้ไม่ประสงค์ดีจะส่งเมลหรือข้อความสนทนาไปในลักษณะที่ไม่เหมาะสมด้วยความคึกคะนอง เช่น ส่งเมลหรือข้อความแชทไปหาเจ้านายของผู้เป็นเจ้าของบัญชีผู้ใช้งานตัวจริงในลักษณะต่อว่า ก็จะทำให้เกิดผลกระทบในเชิงลบขึ้นมาได้เช่นกัน ที่น่ากลัวไปกว่านั้นก็คือการที่ผู้ไม่ประสงค์ดีทำการล็อคอินเข้าไปในระบบแล้วพยายามยกสิทธิ์การใช้งานของตัวเองเพิ่มมากขึ้นตามกรรมวิธีการแฮกเจาะระบบ โดยหากสามารถหาข้อมูลในกลุ่มของผู้ใช้บริการได้มากขึ้นและสามารถยกระดับสิทธิ์การใช้งานได้จนถึงระดับผู้ควบคุมและดูแลระบบ (System Administrator) ข้อมูลทั้งหมดในระบบการให้บริการก็จะตกอยู่ในมือของผู้ไม่ประสงค์ดีได้

๑.๓.๗.๑ การลวงทางเว็บไซต์ อีเมล และโพสต์หรือข้อความแชท

ช่องทางที่นิยมใช้ในการหลอกลวง ได้แก่ **การลวงทางเว็บไซต์** (Website Phishing) **การลวงทางอีเมล** (Email Phishing) และ **การลวงทางโพสต์หรือข้อความแชท** (Social Network Phishing) โดยมักจะทำการหลอกลวงแบบสัมพันธ์กัน ดังนี้

ผู้ไม่ประสงค์ดีจะใช้วิธีการปลอมแปลงเว็บไซต์ (การลวงทางเว็บไซต์) ขึ้นมา โดยทำให้มีลักษณะที่เหมือนกันกับเว็บไซต์จริงอย่างแยกไม่ออก หรือมีลักษณะที่ดูแล้วน่าเชื่อถือว่าเป็นเว็บไซต์จริงของผู้ให้บริการ เช่น สร้างเว็บไซต์ปลอมของ ธนาคาร ผู้ให้บริการอีเมล ผู้ให้บริการการฝากเก็บไฟล์บนคลาวด์ ผู้ให้บริการอื่นออนไลน์ เป็นต้น แล้วสร้างโดเมนเนม (ปรากฏอยู่ใน URL) ที่ดูแล้วสื่อถึงความเป็นเว็บไซต์จริงของผู้ให้บริการ โดยมักมีคำที่ระบุถึงผู้ให้บริการจริงแฝงรวมอยู่ด้วย เพื่อหลอกให้ผู้เปิดเว็บไซต์เชื่อและกรอกข้อมูลสำคัญที่ต้องการลงไป (ภาพที่ ๑.๑๑) โดยจะนำลิงค์ (หลอกลวง) ไปเผยแพร่โฆษณาแฝงตามที่ต่างๆ โดยเฉพาะเว็บท่าประเภทอโคจร ในลักษณะของ Hyperlink ที่หากไม่สังเกตและระมัดระวังให้ดี จะไม่ทราบว่าเมื่อกดที่ลิงค์แล้วจะเชื่อมต่อไปยังที่ใด นอกจากนี้ ยังแฝงส่งลิงค์ (หลอกลวง)ไปกับข้อความในอีเมล (การลวงทางอีเมล) ตลอดจนสื่อการโพสต์หรือแชทต่างๆ (การลวงทางโพสต์หรือข้อความแชท) ในโลกเครือข่ายสังคมออนไลน์อีกด้วย หากผู้ใช้บริการไม่สังเกตและมีความระมัดระวังที่เพียงพอ ก็จะตกเป็นเหยื่อของกลุ่มมิจฉาชีพพวกนี้ได้โดยง่าย



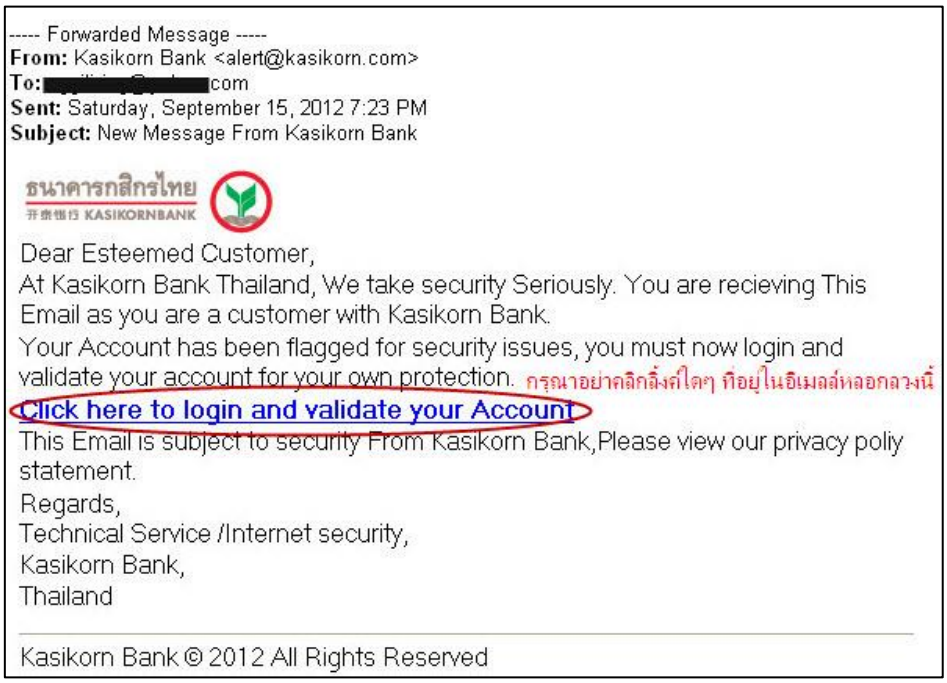
ภาพจาก www.kasikornbank.com

ภาพที่ ๑.๑๑ ตัวอย่างการลวงทางเว็บไซต์ (Website Phishing)

ส่วนใหญ่ที่พบมักจะเป็นการหลอกลวงแบบไม่หวังผลเฉพาะ ในลักษณะของการแอบแฝงส่งลิงค์หลอกลวงไปยังผู้คนจำนวนมากเท่าที่จะหาชื่อบัญชีผู้ใช้บริการประเภทต่างๆ มาได้ และรอคอยการติดกับดักของกลุ่มคนที่ขาดความระมัดระวังมาหลงเชื่อแล้วกรอกข้อมูลสำคัญส่งกลับมาให้ แต่จากผลการสำรวจวิจัยเกี่ยวกับพฤติกรรมการใช้งานอินเทอร์เน็ตและเครือข่ายสังคมออนไลน์

ของกลุ่มผู้บริหารระดับสูงที่มักจะอยู่ใน Baby Boomer Generation (เกิดช่วงปี ค.ศ.๑๙๔๖-๑๙๖๔) และผู้บริหารระดับกลางที่มักจะอยู่ใน X Generation (เกิดช่วงปี ค.ศ.๑๙๖๕-๑๙๘๐) พบว่า สองกลุ่มนี้มีความรู้เท่าทันหรือระแวดระวังภัยอันตรายออนไลน์ค่อนข้างน้อย ทำให้ตกเป็นกลุ่มเป้าหมายของการหลอกลวง และถือเป็นประเภทหลอกลวงแบบเฉพาะเจาะจง (Spear Phishing) ที่มุ่งเป้าเฉพาะไปที่บุคคลสำคัญระดับสูงขององค์กร โดยผลกระทบจะเกิดมากในกรณีนี้ เนื่องจากว่าผู้บริหารระดับสูงจะเกี่ยวข้องกับข้อมูลที่สำคัญๆเป็นจำนวนมาก อีกทั้งยังมักเป็นกลุ่มที่มีสิทธิ์ในการเรียกดูข้อมูลสำคัญๆต่างๆขององค์กรได้ทั้งหมดอีกด้วย

การสังเกตการหลอกลวงคือ หากมีอีเมล ข้อความ โพสต์ ฯลฯ เข้ามาแจ้งให้เปิดลิงค์ตามที่ระบุ (ภาพที่ ๑.๑๒) และให้กรอกข้อมูลชื่อบัญชีผู้ใช้งานกับรหัสผ่าน (และข้อมูลบัตรเครดิต) เพื่อยืนยันการใช้งานอีกครั้ง อันเนื่องมาจากการปรับปรุงเครื่องแม่ข่าย ฯลฯ ให้ระมัดระวังไว้ก่อนเสมอ เพราะโดยปกติผู้ให้บริการจริงจะมีระบบสำรองข้อมูลบัญชีของผู้ใช้งานทั้งหมดไว้เสมอโดยไม่ต้องร้องขอให้กรอกข้อมูลเพื่อยืนยันใดๆ นอกจากนี้ อาจใช้วิธีการโทรศัพท์ (หรือติดต่อด้วยช่องทางการสื่อสารอื่นที่เป็นคนละช่องทางกับช่องทางที่สงสัยว่าได้รับเรื่องหลอกลวงเข้ามา) ติดต่อไปยังผู้ให้บริการแล้วสอบถามถึงเรื่องความจำเป็นในการกรอกข้อมูล ประกอบด้วยอีกทางหนึ่ง ก็จะมีความปลอดภัยเพิ่มขึ้น



----- Forwarded Message -----
From: Kasikorn Bank <alert@kasikorn.com>
To: [redacted]com
Sent: Saturday, September 15, 2012 7:23 PM
Subject: New Message From Kasikorn Bank

ธนาคารกสิกรไทย
开泰银行 KASIKORNBANK

Dear Esteemed Customer,
At Kasikorn Bank Thailand, We take security Seriously. You are recieving This Email as you are a customer with Kasikorn Bank.
Your Account has been flagged for security issues, you must now login and validate your account for your own protection. กรุณาอย่าคลิกลิ้งค์ใดๆ ที่อยู่ในอีเมลล์หลอกลวงนี้
Click here to login and validate your Account
This Email is subject to security From Kasikorn Bank,Please view our privacy poliy statement.
Regards,
Technical Service /Internet security,
Kasikorn Bank,
Thailand

Kasikorn Bank © 2012 All Rights Reserved

ภาพจาก www.kasikornbank.com

ภาพที่ ๑.๑๒ ตัวอย่างการลวงทางอีเมล (Email Phishing)

แนวทางการป้องกันการหลอกลวง (Phishing) สามารถปฏิบัติได้ ดังนี้

๑) ไม่คลิกลิงค์ที่แนบมากับอีเมลหรือห้องสนทนาออนไลน์โดยตรง ให้พิมพ์ค่า URL ใหม่โดยตรง หรือเข้าจากเว็บที่เป็นทางการของผู้ให้บริการเท่านั้น

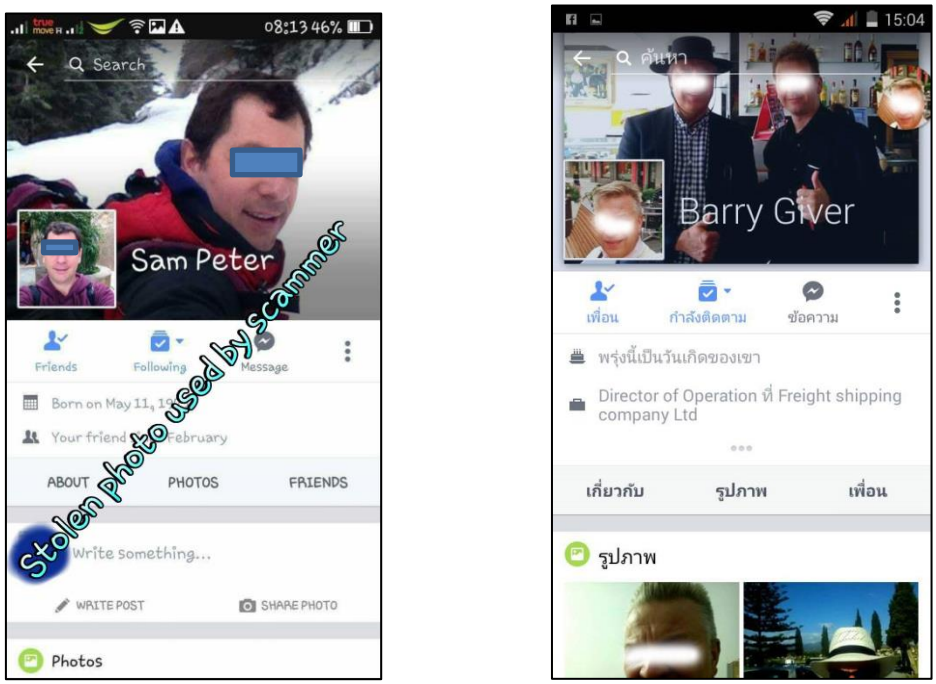
๒) ไม่เชื่อข้อความในอีเมลหรือห้องสนทนาออนไลน์ที่ให้กรอกค่ารหัสผ่านหรือข้อมูลสำคัญ เพื่อยืนยันการรับบริการ/สถานภาพการใช้งาน หรือให้ทำธุรกรรมการเงินในรูปแบบใดๆ ให้ตรวจสอบกับผู้ให้บริการด้วยช่องทางที่เป็นทางการอื่นประกอบด้วยทุกครั้ง

๓) ไม่หลงเชื่อให้ข้อมูลสำคัญส่วนบุคคลกับการร่วมสนุกแบบออนไลน์ต่างๆ

๑.๓.๗.๒ การลวงแบบสแคมเมอร์ (Scammer)

สแคมเมอร์ (Scammer) เป็นรูปแบบการลวงชนิดหนึ่ง ที่มุ่งเป้าไปที่การหลอกลวงให้ผู้ที่ตกเป็นเหยื่อหลงเชื่อและไว้ใจ หลังจากนั้นจะทำการหลอกลวงเพื่อพยายามเอาเงินจากเหยื่อในลักษณะต่างๆ และเมื่อได้เงินแล้วก็จะจากหายไป โดยส่วนใหญ่พบว่าเป็นปฏิบัติการหลอกลวงของชาวต่างชาติที่อาศัยความโลภของเหยื่อเป็นสำคัญ และการสนทนามักจะเป็นภาษาอังกฤษที่มีความสุภาพน่าเชื่อถือ แบ่งเป็น ๒ ลักษณะด้วยกัน ได้แก่ สแคมเมอร์ทั่วไป (Scammer) และสแคมเมอร์โรแมนติก (Romance Scammer) โดยทั้ง ๒ ลักษณะจะมีขั้นตอนการปฏิบัติการแบ่งออกเป็น ๓ ขั้นตอน ดังนี้

๑) ขั้นทำความรู้จัก เป็นขั้นตอนที่ผู้ไม่ประสงค์ดีจะส่งคำร้องขอเป็นเพื่อนไปทางสื่อสังคมออนไลน์ชนิดต่างๆ เช่น Facebook และ LINE โดยจะใช้รูป Profile ปลอม ที่ดูดีและน่าเชื่อถือ (ภาพที่ ๑.๑๓) เป็นสิ่งล่อให้ปลายทางกดรับคำร้องขอเพื่อเป็นเพื่อนในสังคมออนไลน์ หลังจากนั้นก็จะทักทายเข้ามาทางช่องทางส่วนตัว (เช่น Inbox) เพื่อขอพูดคุยด้วย โดยจะเพิ่มความถี่ในการสนทนามากขึ้นเป็นลำดับ เพื่อสร้างความคุ้นเคยให้เกิดขึ้นโดยเร็ว และมีการถามข้อมูลส่วนบุคคลเพื่อการติดต่อ เช่น หมายเลขโทรศัพท์และที่อยู่ เป็นต้น ทั้งนี้ สแคมเมอร์โรแมนติก (Romantic Scammer) จะเลือกเป้าหมายที่เป็นเพศตรงข้าม



ภาพที่ ๑.๑๓ ตัวอย่างชื่อและรูป Profile ปลอมที่ใช้ในการลวงแบบสแคมเมอร์

๒) ขั้นแอบอ้าง เป็นขั้นตอนที่ผู้ไม่ประสงค์ดีจะพูดคุยแอบอ้าง เพื่อให้เหยื่อเกิดความเชื่อถือและตายใจ โดยมุ่งเป้าไปที่การใช้ความโลภของเหยื่อเป็นตัวหลอกล่อ ดังนี้

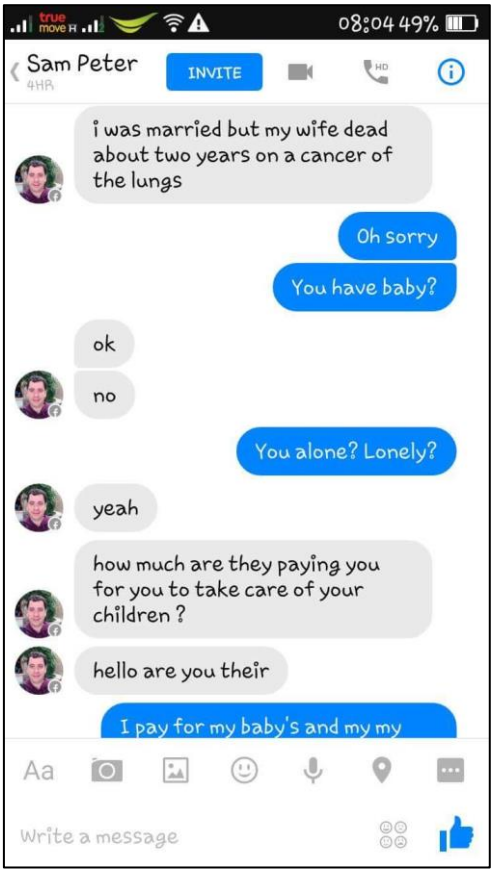
สแคมเมอร์ทั่วไป (Scammer) : จะแอบอ้างว่าตนเองประกอบธุรกิจขนาดใหญ่ที่มีมูลค่าสูง เช่น ธุรกิจนำเข้าและส่งออกอุปกรณ์ IT, อัญมณี, ของเก่าล้ำค่า และนาฬิกายี่ห้อดังต่างๆ เป็นต้น หรืออยากจะมาลงทุนธุรกิจในประเทศของเหยื่อ (ภาพที่ ๑.๑๔)

ภาพที่ ๑.๑๔ ตัวอย่างข้อความอ้างว่าอยากลงทุนที่ใช้ในการลวงแบบสแคมเมอร์

สแคมเมอร์โรแมนติก (Romance Scammer) : จะแอบอ้างว่าตนเองยังโสดหรือสามี/ภรรยาเสียชีวิต และหลงชอบ/หลงรักเหยื่อ และแสดงความรักใคร่ชอบพอออกมาอย่างรวดเร็วและชัดเจน โดยจะเน้นว่าอยากคบหาดูแลและแต่งงานด้วยอย่างจริงจังในเวลาอันรวดเร็ว (ภาพที่ ๑.๑๕)

๓) ขั้นหลอกลวง เป็นขั้นตอนที่ผู้ไม่ประสงค์ดีจะแจ้งเหยื่อว่าตนเองจะส่งของต่างๆ มาให้จากต่างประเทศหรือจากแหล่งอื่น ซึ่งเป็นของที่มีมูลค่าสูง หลังจากนั้น จะมีทีมปฏิบัติการเดียวกัน โทรศัพท์ติดต่อมายังเหยื่อ พร้อมแจ้งว่ามีของมูลค่าสูงถูกส่งมาจากต่างประเทศหรือแหล่งอื่น แต่เนื่องจากเป็นของที่มีมูลค่าสูงจึงจำเป็นที่เหยื่อจะต้องชำระภาษีศุลกากร ฯลฯ ก่อนด้วยการโอนเงินตามขั้นตอนที่กำหนด (ขั้นตอนปลอม เพื่อดึงเงินไปยังบัญชีของผู้ไม่ประสงค์ดี) เพื่อที่จะได้นำของนั้นออกและจัดส่งให้เหยื่อตามที่อยู่ที่ระบุไว้ (ผู้ไม่ประสงค์ดีจะหลอกถามข้อมูลนี้ไว้

แล้วในขั้นตอนที่ ๑) ต่อไป และยังมีลักษณะที่พยายามรวบรัดและเร่งรัดการโอนเงิน ซึ่งสแคมเมอร์จะใช้ประโยชน์จากความโลภของเหยื่อ ประกอบกับรูปการณ์ที่สอดคล้อง เนื่องจากมีการแจ้งเหยื่อว่าจะส่งของให้ และหลังจากนั้นก็มีการติดต่อจากเจ้าหน้าที่ไปยังเหยื่อพร้อมแจ้งว่ามีของนั้นถูกส่งมาให้ นอกจากนี้ยังพบว่ามีลักษณะของการหลอกลวงว่าจะเข้ามาลงทุนทำธุรกิจขนาดใหญ่ในประเทศของเหยื่ออีกด้วย ทำให้มีผู้คนเป็นจำนวนไม่น้อยที่ตกเป็นเหยื่อของเหล่าสแคมเมอร์นี้ (ภาพที่ ๑.๑๖)



ภาพที่ ๑.๑๕ ตัวอย่างข้อความอ้างว่าอยากคบหาดูแลที่ใช้ในการลวงแบบสแคมเมอร์

ภาพที่ ๑.๑๖ ตัวอย่างข่าวผู้ถูกลวงแบบสแคมเมอร์

แนวทางในการป้องกันการลวงแบบสแคมเมอร์ (Scammer) แบ่งแยกตามขั้นตอนการปฏิบัติการ ดังนี้

๑) ขั้นทำความรู้จัก ให้สังเกตและตรวจสอบประวัติของผู้ที่ส่งคำร้องขอเป็นเพื่อทางสังคมออนไลน์ก่อนกดรับคำร้องขอทุกครั้ง โดยให้ทำการตรวจสอบระยะเวลาในการเริ่มทำกิจกรรมออนไลน์ ประวัติการโพสต์ และกลุ่มเพื่อนของผู้ที่ร้องขอเข้ามา โดยพบว่าสแคมเมอร์ (Scammer) จะใช้ชื่อบัญชี (User Account) ที่เพิ่งสร้างขึ้นชั่วคราวไม่นาน ใช้รูป Profile ของผู้อื่นที่ดูดีน่าเชื่อถือหรือดูหน้าตาและการแต่งกายดี มีประวัติการโพสต์ที่น้อยมาก และมีกลุ่มเพื่อนในสังคมออนไลน์เพียงไม่กี่คน

๒) ขั้นแอบอ้าง ให้สังเกตว่า สแคมเมอร์ทั่วไป (Scammer) จะเป็นลักษณะของการแอบอ้างเกินจริง เช่น มีการส่งรูปที่ถือเงินเป็นจำนวนมาก รูปที่นั่งรถสปอร์ต รูปกับบ้านหลังใหญ่ และสแคมเมอร์โรแมนติก (Romance Scammer) จะเป็นลักษณะของการแสดงการหลงรักอย่างหมดหัวใจ ใช้คำสรรพนามเรียกอีกฝ่ายว่าที่รัก (Darling) ในเวลาอันรวดเร็ว หรือแสดงให้เห็นว่าเป็นรักแรกพบหรือรักที่รอคอยมานาน

๓) ขั้นหลอกลวง ให้สังเกตและตรวจสอบทุกครั้งที่มีการแจ้งส่งของหรือพัสดุใดๆ โดยให้พึงระวังไว้ก่อนว่า การขอให้มีการโอนเงินเพื่อเป็นค่าใดๆ ก็ตาม จะมีความเสี่ยงต่อการถูกหลอกลวงเสมอ และในการตรวจสอบ ไม่ใช้หมายเลขโทรศัพท์ที่ได้รับแจ้ง แต่ใช้หมายเลขโทรศัพท์ที่เป็นทางการของหน่วยงานตามที่ได้รับแจ้ง ในการตรวจสอบเท่านั้น

สรุปการลวงแบบสแคมเมอร์ (Scammer) แสดงดังตารางที่ ๑.๑

ตารางที่ ๑.๑ สรุปการลวงแบบสแคมเมอร์

ขั้นตอน	๑. ทำความรู้จัก	๒. แอบอ้าง	๓. หลอกลวง
รูปแบบ	- ส่งคำร้องขอเป็นเพื่อน - รูป Profile ดูดี	- ประกอบธุรกิจ - มีฐานะดี - บอกรัก/ขอแต่งงาน	- ส่งของ (มูลค่าสูง) มาให้ - ต้องมีค่าใช้จ่ายในการนำของออก - ให้โอนเงิน
ข้อสังเกต	- เป็นบัญชีที่เปิดใช้งานไม่นาน - ประวัติการโพสต์น้อย - มีกลุ่มเพื่อนออนไลน์น้อย	- อวดอ้างความร่ำรวยเกินจริง - บอกรัก/ขอแต่งงาน อย่างรวดเร็ว	- แหล่งที่ติดต่อมาไม่ชัดเจน - ตรวจสอบไปยังหน่วยงานจริง - รวบรัด/เร่งรัด การโอนเงิน

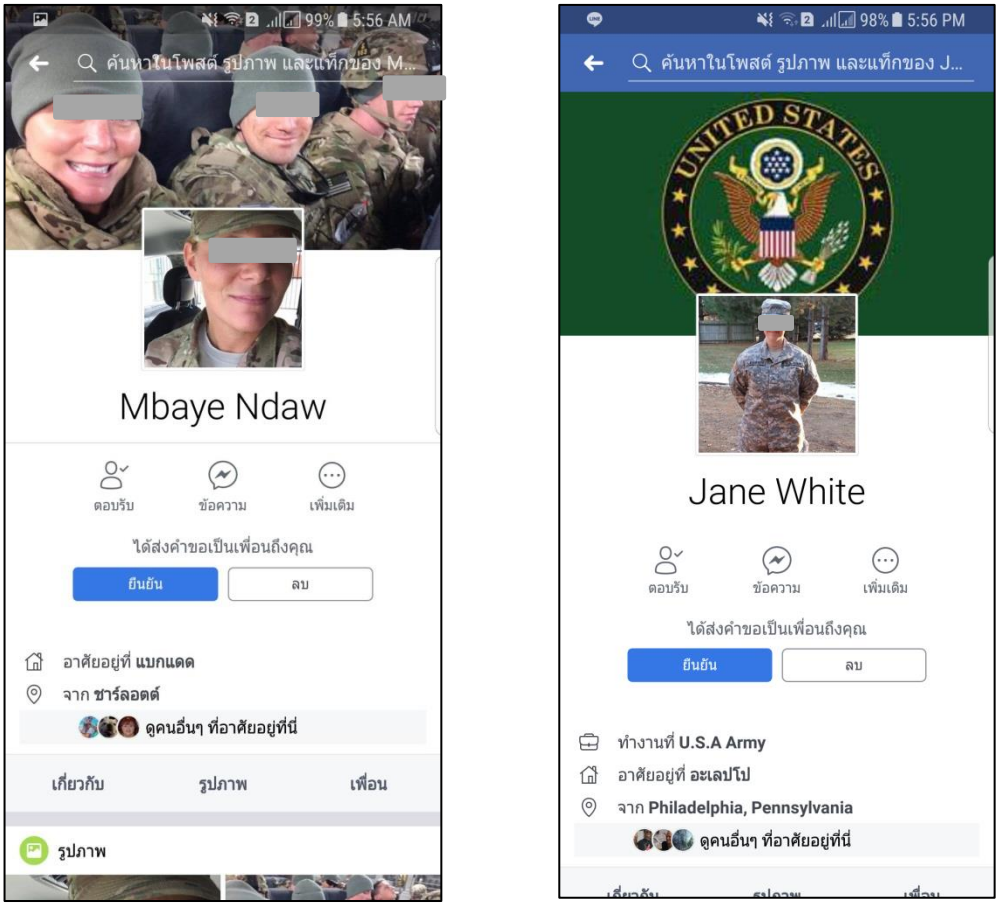
๑.๓.๗.๓ การลวงเพื่อการขู่เรียกร้องเงิน (Blackmail)

การลวงประเภทนี้ มีลักษณะคล้ายกับสแคมเมอร์ (Scammer) ในขั้นตอนที่ ๑ คือ การพยายามส่งคำร้องขอเป็นเพื่อนทางสังคมออนไลน์ไปยังเป้าหมาย ซึ่งส่วนใหญ่เป็นปฏิบัติการของผู้ไม่ประสงค์ดีที่อ้างตัวเป็นเพศหญิง โดยใช้รูป Profile ที่หน้าตาดีและมีความอีโรติกเพื่อดึงดูดให้เป้าหมายที่เป็นเพศชายกดรับคำร้องขอ หลังจากนั้นก็จะเข้าสู่ขั้นตอนที่ ๒ คือการพยายามชักชวนให้เป้าหมายร่วมสนทนาแบบส่วนบุคคล ซึ่งจะมีการส่งรูปเพิ่มเติมและพยายามชักชวนให้เป้าหมายร่วมสนทนาแบบ VDO Call เช่น ผ่าน Spype เป็นต้น

เมื่อปลายทางหลงเชื่อ มีการสนทนาแลกเปลี่ยนรูปภาพทางช่องทางสื่อสารส่วนบุคคลเพิ่มขึ้น หรือมีการสนทนาแบบ VDO Call ก็จะแอบแทรกส่งรูปภาพโป๊เปลือย หรือส่งเป็น VDO ภาพโป๊เปลือยเข้ามา โดยทั้งหมดจะถูกบันทึกการสนทนาไว้ และเมื่อเหยื่อมีการโต้ตอบในเชิงร่วมสนุกอย่างใดก็ตาม ผู้ไม่ประสงค์ดีจะบันทึกพฤติกรรมนั้น แล้วนำมาข่มขู่เรียกร้องเงิน เพื่อแลกกับการไม่เปิดเผยครลิปการบันทึกนั้นๆ

โดยส่วนใหญ่จะมีการสำรวจและเลือกเป้าหมายที่เป็นผู้มีหน้าที่การงานในสังคมที่ดี เนื่องจากหากการปฏิบัติการสำเร็จ มีแนวโน้มสูงที่เหยื่อจะยอมจ่ายเงินเพื่อแลกกับการไม่เปิดเผยคลิปพฤติกรรมที่ไม่พึงประสงค์ของตนเอง

ทั้งนี้ ผู้ไม่ประสงค์ดีจะมีการสำรวจข้อมูลของเป้าหมายก่อน แล้วพยายามสร้างบัญชีผู้ใช้ (User Account) ที่มีอาชีพในแวดวงใกล้เคียงกับเป้าหมาย เพื่อให้เป้าหมายกดรับเพิ่มเป็นเพื่อนได้เร็วขึ้น เช่น ใช้รูป Profile เป็นทหารหญิงต่างชาติ เพื่อส่งคำร้องมายังกำลังพลทหารชาย (ภาพที่ ๑.๑๗)



ภาพที่ ๑.๑๗ ตัวอย่างคำร้องขอเป็นเพื่อนจากผู้ที่ไม่รู้จัก

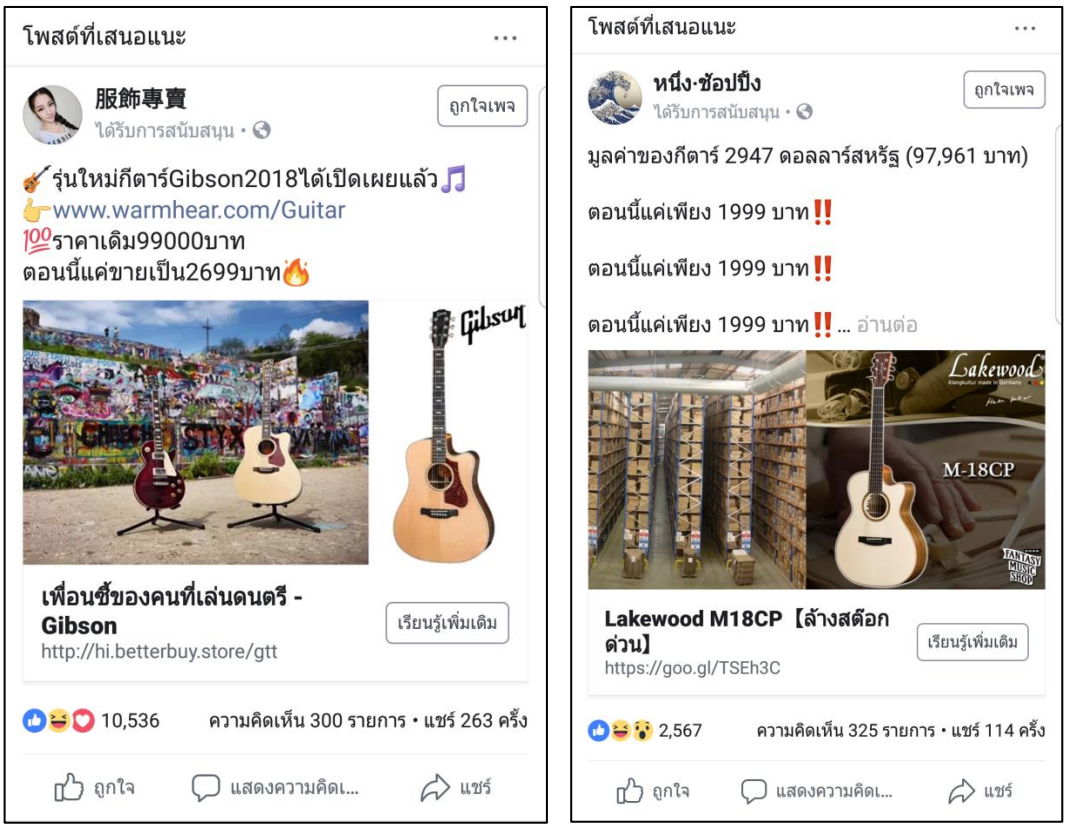
๑.๓.๗.๔ การลวงด้วยการโฆษณาสินค้าปลอมที่ราคาถูกเกินจริง

เป็นรูปแบบการลวงในสังคมออนไลน์ที่ผู้ไม่ประสงค์ดีจะใช้วิธีตั้งร้านค้าออนไลน์ขึ้นมา แล้วนำเสนอขายสินค้าที่ได้รับความนิยมต่างๆ เช่น กระเป๋า นาฬิกา และเครื่องดนตรี เป็นต้น ในราคาที่ถูกมากเกินจริง โดยเมื่อมีเหยื่อสั่งสินค้า ก็จะจัดส่งสินค้าที่ด้อยคุณภาพหรือไม่เป็นไปตามที่โฆษณาให้แทน ซึ่งรูปแบบในการส่งสินค้า มีทั้งที่ต้องชำระค่าสินค้าก่อนล่วงหน้า และแบบเก็บเงินปลายทาง หรือหลอกเก็บข้อมูล ชื่อ ที่อยู่ และหมายเลขโทรศัพท์ โดยไม่มีการจัดส่งสินค้า

อย่างไรก็ดี ในการจัดส่งแบบเก็บเงินปลายทาง ผู้รับสินค้ามักจะชำระค่าสินค้าก่อนที่จะเปิดดูสินค้าจริง ทำให้มีผู้เสียหายเป็นจำนวนมากที่ตกเป็นเหยื่อการลวงในลักษณะนี้

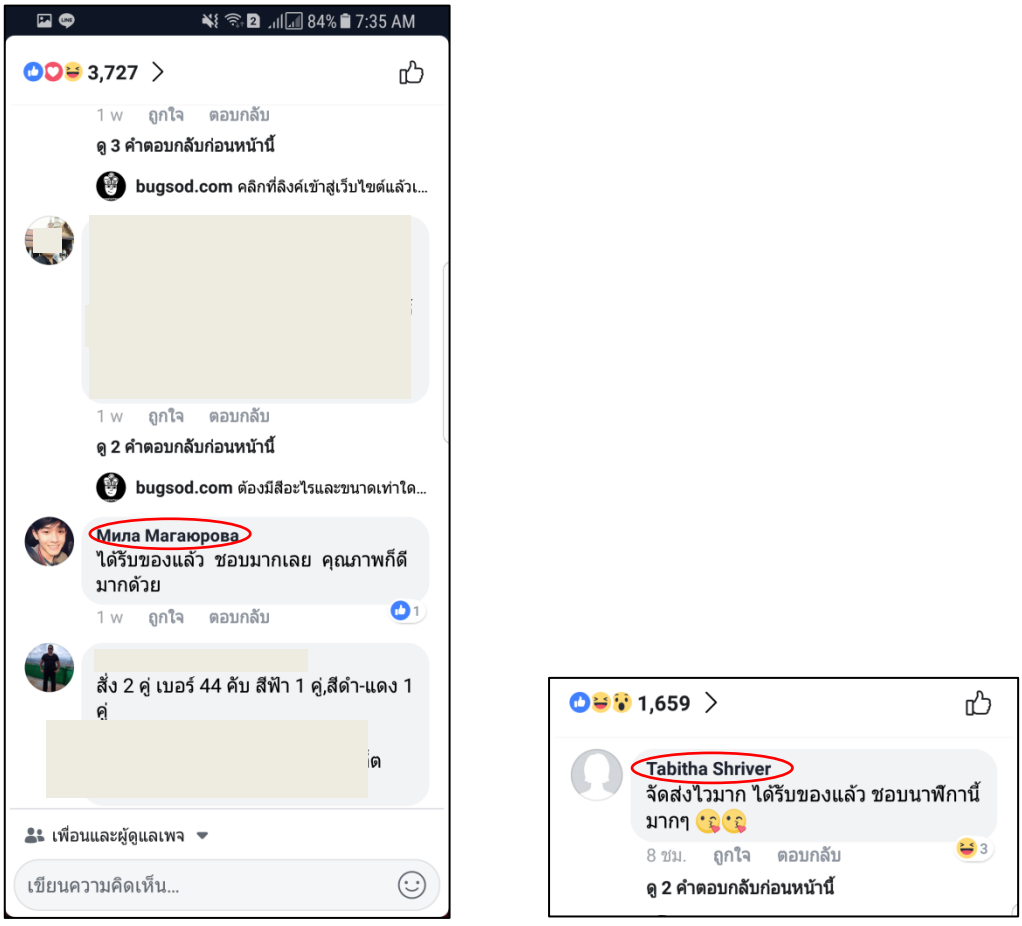
ที่น่ากลัวไปกว่านั้นก็คือ การที่ร้านค้าออนไลน์ต่างๆ เหล่านี้ได้ลงทุนซื้อโฆษณาจากผู้ให้บริการเครือข่ายสังคมออนไลน์ เล่น Facebook ทำให้หน้าร้านถูกโพสต์ขึ้นเป็น **ร้านค้าแนะนำ** หรือ **โพสต์ที่เสนอแนะ** ใน Facebook ทำให้มีผู้หลงเชื่อและตกเป็นเหยื่อเป็นจำนวนมาก (ภาพที่ ๑.๑๘)

นอกจากนี้ ยังพบว่ามีเทคนิคในการลงคอมเม้นต์ (Comment) ชื่นชมสินค้าปลอมในลักษณะของหน้าม้า เพื่อเพิ่มความน่าเชื่อถืออีกด้วย โดยจุดนี้สามารถสังเกตได้ง่ายจากการที่ผู้โพสต์เป็นชื่อบัญชีชาวต่างชาติ แต่โพสต์ข้อความชื่นชมสินค้าเป็นภาษาไทย ซึ่งพบอีกว่าภาษาที่ใช้ทั้งในการโฆษณาและคอมเม้นต์สนับสนุนนั้น เป็นลักษณะของภาษาไทยที่ใช้โปรแกรมแปลภาษามา (ภาพที่ ๑.๑๙) ทำให้เกิดข้อสังเกตและการถามตอบที่ผิดธรรมชาติของภาษาไทยขึ้น (ภาพที่ ๑.๒๐)

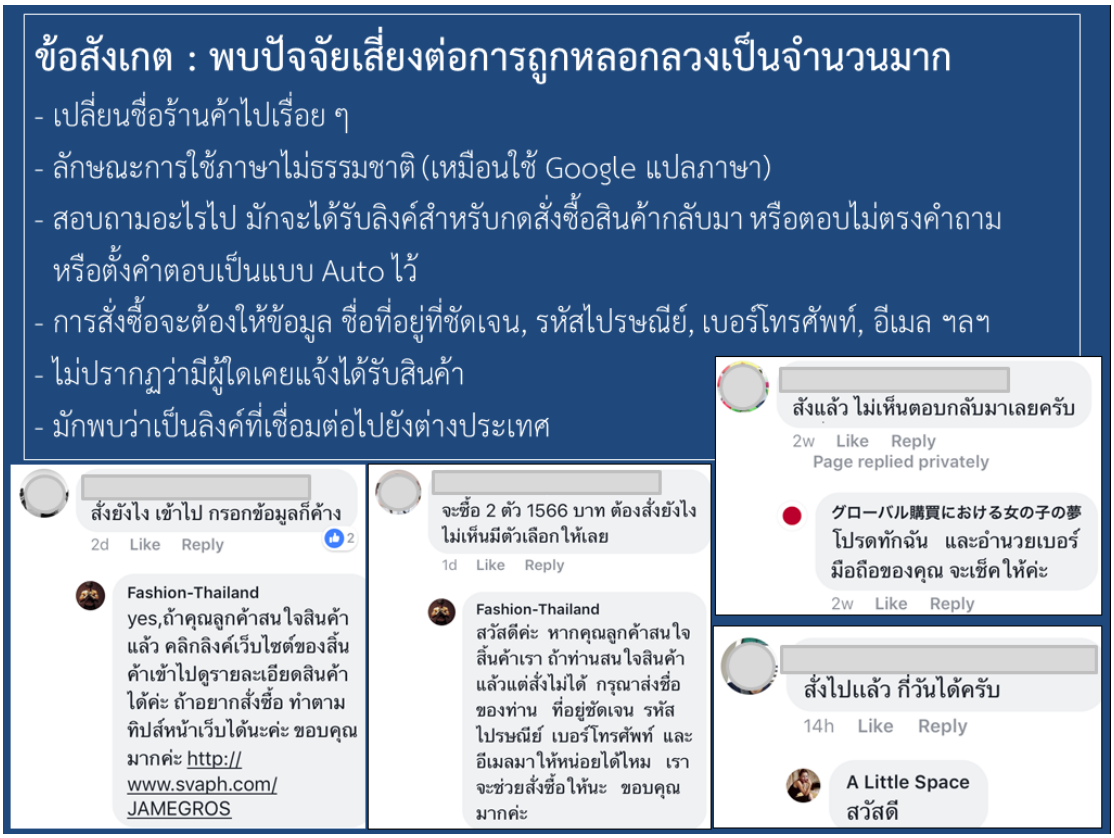


ภาพที่ ๑.๑๘ ร้านค้าออนไลน์ที่เสนอขายสินค้าราคาถูกเกินจริง

ภาพที่ ๑.๑๘ ร้านค้าออนไลน์ที่เสนอขายสินค้าราคาถูกเกินจริง (ต่อ)



ภาพที่ ๑.๑๙ โพสต์ข้อความแบบหน้าม้าที่สนับสนุนหรือชื่นชมสินค้า



ภาพที่ ๑.๒๐ ข้อสังเกตและการถามตอบที่ผิดธรรมชาติของภาษาไทย

๑.๓.๗.๕ การลวงในลักษณะของแก๊งคอลเซ็นเตอร์ (Call Center)

เป็นการลวงผ่านการโทรศัพท์ไปยังเป้าหมาย โดยแอบอ้างเป็นเจ้าหน้าที่ของหน่วยงาน แล้วแจ้งข้อขัดข้องต่างๆ ที่เกิดให้ทราบ และชัดจูงให้ปฏิบัติตามขั้นตอนที่กำหนดเพื่อทำการแก้ไขปัญหาที่เกิดขึ้น โดยมักจะพบว่าเป็นการเรียกร้องให้ทำธุรกรรมการเงินเพื่อให้เงินเข้าไปยังผู้ไม่ประสงค์ดี เช่น

๑) แก๊ง Call Center แอบอ้างเป็น บริษัท ทีโอที จำกัด (มหาชน) แจ้งว่าสัญญาณโทรศัพท์จะถูกระงับ โดยจะมีเสียงอัตโนมัติในลักษณะที่ว่า “ทีโอที สวัสดีค่ะ ขณะนี้สัญญาณโทรศัพท์ของคุณจะถูกระงับภายใน ๒ ชั่วโมง กด ๑ เพื่อติดต่อสอบถามพนักงาน” เมื่อรับสายและกดตามข้อความเสียง อาจตกเป็นเหยื่อ ถูกหลอกถามชื่อ, เลขที่บัตรประชาชน, ข้อมูลสำคัญส่วนบุคคล หรือหลอกให้ทำธุรกรรมการเงินได้

๒) แก๊ง Call Center แอบอ้างเป็นไปรษณีย์ไทยแจ้งว่ามีพัสดุตกค้าง โดยจะมีเสียงอัตโนมัติในลักษณะที่ว่า “ท่านมีพัสดุที่ยังไม่ได้รับจากไปรษณีย์ไทย กรุณากด ๙ เพื่อสอบถามรายละเอียด” เมื่อรับสายและกดตามข้อความเสียง อาจตกเป็นเหยื่อ ถูกหลอกถามชื่อ, เลขที่บัตรประชาชน, ข้อมูลสำคัญส่วนบุคคล หรือหลอกให้ทำธุรกรรมการเงินได้

๓) แก๊ง Call Center ต่างประเทศแอบอ้างเป็นบริษัทไปรษณีย์ไทย แจ้งว่ามีพัสดุตกค้าง หรือแอบอ้างเป็นบริษัทผู้ให้บริการเครือข่ายโทรศัพท์ แจ้งว่าค้างชำระค่าบริการกำลังจะถูกระงับสัญญาณ หรือแจ้งว่ามีการนำสำเนาบัตรประชาชนของเราไปเปิดเบอร์ใหม่ และให้กด ๑ เพื่อติดต่อเจ้าหน้าที่ โดยพบว่าหมายเลข ๐-๓๑๗๔-๓๑๗๘ และ ๐-๒๐๒๒-๗๑๑๐ เป็นตัวอย่างของหมายเลขที่มีพฤติการรมการหลอกลวงในลักษณะนี้ เมื่อรับสายและกดตามข้อความเสียง อาจตกเป็นเหยื่อ ถูกหลอกถามชื่อ, เลขที่บัตรประชาชน, ข้อมูลสำคัญส่วนบุคคล หรือหลอกให้ทำธุรกรรมการเงินได้

๑.๓.๗.๖ การลวงเรื่องสร้างรายได้จากการทำงานผ่านอินเทอร์เน็ต

เป็นลักษณะการโฆษณาชวนเชื่อ เพื่อหลอกลวงว่าสามารถทำงานหารายได้เป็นจำนวนมากจากการทำงานผ่านอินเทอร์เน็ต (ภาพที่ ๑.๒๑)

ภาพที่ ๑.๒๑ โฆษณาการหารายได้จากการทำงานผ่านอินเทอร์เน็ต

เนื้อหาการโฆษณาประชาสัมพันธ์และเชื้อเชิญให้ร่วมทำงานพิเศษผ่านระบบอินเทอร์เน็ต ด้วยการคลิกเพื่อส่งข้อมูล หรือเปิดดูหน้าเว็บไซต์ต่างๆ เพื่อเพิ่มจำนวนผู้เข้าชมหน้าเว็บนั้นๆ ให้มากขึ้น แล้วจะได้ค่าตอบแทนเป็นเงินโอนเข้าบัญชี ในจำนวนที่เรียกว่าสูงเมื่อเทียบกับการคลิกและเวลาที่จะต้องเสียไป เป็นสิ่งที่สามารถพบเห็นได้บ่อยครั้งในเกือบจะทุกช่องทางที่ข้อมูลประชาสัมพันธ์จะเข้าถึงและไปปรากฏตัวได้ ไม่ว่าจะลงในหน้าเว็บเพจโฆษณา ส่งผ่านอีเมล หรือแม้กระทั่งส่งไปลงในเครือข่ายสังคมออนไลน์ เช่น Facebook เป็นต้น

การทำงานผ่านอินเทอร์เน็ต แบ่งออกเป็น ๒ รูปแบบด้วยกัน คือ ๑) การคลิกเพื่อเพิ่มยอดผู้เข้าชมในโฆษณาต่างๆ และ ๒) การแอบแฝงการทำธุรกรรมแบบลูกโซ่ โดยมีรายละเอียดของแต่ละรูปแบบ ดังนี้

๑) การคลิกเพื่อเพิ่มยอดผู้เข้าชมในโฆษณาต่างๆ

การสร้างรายได้จากการคลิกเพื่อเข้าชมสื่อโฆษณาประชาสัมพันธ์ต่างๆ เป็นสิ่งที่มองได้ว่ามีความสมเหตุสมผลและมีความเป็นไปได้ เนื่องจากการเข้าชมโฆษณาประชาสัมพันธ์ต่างๆ เป็นการสร้างโอกาสด้านการขายให้กับเจ้าของผลิตภัณฑ์ จึงมีความเป็นไปได้และเหมาะสมที่จะได้อะไรเป็นสิ่งตอบแทน ซึ่งที่จริง งานในลักษณะเช่นนี้มีมานานพอสมควรแล้ว ตั้งแต่ยุคที่อินเทอร์เน็ตเริ่มเข้ามาใหม่ๆ ในลักษณะที่บริษัทผู้ผลิตสินค้าต่างๆ (โดยเฉพาะบริษัทต่างประเทศ) ว่าจ้างให้เอเย่นต์โฆษณาเป็นผู้ผลิตงานโฆษณาสินค้าของบริษัท และจัดเผยแพร่สื่อผลงานโฆษณานั้นต่อผู้คนทางช่องทางอินเทอร์เน็ตเพื่อการประชาสัมพันธ์สินค้าต่างๆ ดังกล่าว พร้อมตั้งเงื่อนไขการจ่ายเงินค่าตอบแทนให้กับเอเย่นต์ในกรณีที่โฆษณาสินค้านั้นๆ ได้รับการเปิดดูทางอินเทอร์เน็ตโดยผู้บริโภค เช่น หากมีผู้บริโภคคนใดเปิดชมสื่อโฆษณาประชาสัมพันธ์เป็นระยะเวลา ๑ ชั่วโมง ก็จะจ่ายค่าตอบแทนให้กับเอเย่นต์ฯ เป็นจำนวน ๑๐๐ บาท เป็นต้น ตรงนี้ เอเย่นต์ต่างๆ จะระดมส่งเมลหรือโพสต์ลงในอินเทอร์เน็ต เพื่อดึงให้ผู้ที่สนใจจะรับชมสื่อโฆษณาต่างๆ นั้นมาลงทะเบียนสมัครรับชมโดยมีค่าชมเป็นเงินตอบแทน ซึ่งอัตราที่เอเย่นต์จะจ่ายให้กับผู้ที่เปิดโฆษณาชมนั้นจะต่ำกว่าอัตราที่เอเย่นต์จะได้จากบริษัทผู้ผลิตมาก เช่น เปิดชมเป็นระยะเวลา ๑ ชั่วโมง ก็จะจ่ายให้ ๒๐ บาท เป็นต้น แต่อัตรานี้ก็เรียกได้ว่ายังมีแรงจูงใจสูงพอที่จะให้ผู้ที่มีเวลาว่างและเล่นอินเตอร์ในแต่ละวันเป็นระยะเวลานานๆ อยู่แล้ว สนใจจะสมัครเปิดชมสื่อโฆษณาดังกล่าวเพื่อแลกกับเงินค่าตอบแทนซึ่งอาจจะเรียกได้ว่าได้มาฟรี

ในยุคเริ่มแรก ผู้บริโภคที่สนใจจะเข้าชมโฆษณาต่างๆ จะต้องดาวน์โหลดโปรแกรมเล็กๆ ลงในเครื่องคอมพิวเตอร์ของตัวเอง แล้วเปิดขึ้นมาเพื่อรับชมสื่อโฆษณานั้นๆ ผ่านทางอินเทอร์เน็ตระหว่างที่ใช้งานคอมพิวเตอร์ โดยโปรแกรมจะเปิดหน้าต่างเล็กๆ ขึ้นมาบนหน้าจอคอมพิวเตอร์ เพื่อแสดงผลโฆษณาของสินค้าหรือชุดของสินค้า (Product Series) บนหน้าจอคอมพิวเตอร์ ซึ่งเงินค่าตอบแทนในการเปิดชมจะถูกจ่ายตามระยะความยาวของเวลาที่เปิดรับชม แต่มีข้อจำกัดที่ว่า เครื่องคอมพิวเตอร์ดังกล่าวจะต้องกำลังถูกใช้งานโดยผู้ใช้จริงๆ และกระบวนการที่ใช้ในการตรวจสอบว่ากำลังใช้งานอยู่จริงหรือไม่ก็คือ การคอยเฝ้าสังเกตการขยับและการคลิกของเม้าส์โดยตัวโปรแกรมที่โหลดลงในเครื่องคอมพิวเตอร์ กล่าวคือ หากโปรแกรมแสดงสื่อโฆษณาพบว่า เครื่องคอมพิวเตอร์ที่เปิดชมสื่อโฆษณานั้นมีการขยับและมีการคลิกของเม้าส์ภายในระยะเวลาที่กำหนด ก็จะนับเวลาต่อเนื่องให้ แล้วแปลงออกมาเป็นเงินค่าตอบแทนในการชมสื่อโฆษณาให้กับผู้เปิดชม (เป็นตัวเลขที่แสดงให้เห็น) แต่จะมีกำหนดจำนวนเงินขั้นต่ำสุด ที่ผู้ชมสื่อโฆษณาจะสามารถขอเบิกเงินได้ เช่น จะต้องสะสมยอดเงินให้ได้ ๒,๐๐๐ บาทขึ้นไป จึงจะสามารถขอเบิกเงินได้ โดยหากยอดเงินสะสมต่ำกว่านั้นจะต้องเปิดชมสื่อโฆษณาเพิ่มอีก เพื่อสะสมให้ยอดเงินครบตามจำนวนที่กำหนดก่อนจึงจะสามารถขอเบิกได้ (ให้โอนเข้าบัญชีธนาคารของตัวเองที่ลงทะเบียนไว้)

ต่อมา เมื่อมีผู้คิดค้นโปรแกรมโกงเรื่องการเปิดชมสื่อโฆษณา ด้วยการตั้งให้เม้าส์ขยับและคลิกได้เองเพื่อหลอกให้โปรแกรมแสดงสื่อโฆษณานับเวลาและแปลงเป็นยอดเงินให้

แม้ผู้ใช้งานคอมพิวเตอร์จะไม่ได้ใช้งานคอมพิวเตอร์และชมจริงก็ตาม วิธีการจ่ายเงินค่าตอบแทนในการเข้าชมสื่อโฆษณาดังกล่าวจึงได้เปลี่ยนรูปแบบไปเป็นการคลิกที่แบนเนอร์โฆษณาต่างๆ เพื่อเข้าไปเปิดชมจากเว็บไซต์ของผู้ผลิตโดยตรง (แทนการเปิดโปรแกรมเล็กๆ แล้วรอรับชมบนหน้าจอ) โดยอัตราค่าตอบแทนเป็นตัวเงินจะจ่ายตามจำนวนการคลิกเข้าไปชม แทนการจ่ายตามระยะความยาวของเวลาที่เปิดชม เช่น หากมีผู้บริโภคคนใดคลิกเข้าชมสื่อโฆษณาประชาสัมพันธ์เป็นจำนวน ๑๐,๐๐๐ ครั้ง เอเย่นต์ก็จะได้ค่าตอบแทน เป็นจำนวนเงิน ๑,๐๐๐ บาท จากบริษัทผู้ผลิต เป็นต้น ซึ่งมีคำถามคือ แล้วผู้คลิก (ให้กับเอเย่นต์) จะได้รับเงินค่าตอบแทนจริงหรือไม่

คำตอบคือ มีระบุไว้ในค่าตอบแทนจริง (บางแห่งเป็นเครดิตเงินสำหรับให้ลงโฆษณา) แต่จำนวนครั้งในการคลิกขั้นต่ำ (คลิกเปิดดูแบนเนอร์) เพื่อให้ได้มาซึ่งเงินค่าตอบแทนนั้นมีจำนวนมากและใช้เวลานาน อีกทั้งอัตราค่าตอบแทนในการคลิกก็เรียกได้ว่าน้อยมาก ดังนั้น คนที่จะได้เงินค่าตอบแทนสูงตามคำโฆษณา (ชวนเชื่อ) จึงเป็นไปได้ยากมากในเชิงปฏิบัติ เช่น ต้องคลิกขั้นต่ำถึงจำนวน ๑,๐๐๐ ครั้ง จึงจะได้ค่าตอบแทน ๑๐ บาท (อัตรา ๑ สตางค์ ต่อ ๑ คลิก) เป็นต้น นอกจากนี้ การคลิกให้ได้ครบตามจำนวนครั้งขั้นต่ำดังกล่าวอาจจะมีระบุระยะเวลา (Session Time) เอาไว้ด้วย โดยภายในระยะเวลาที่กำหนด หากคลิกไม่ถึงจำนวนขั้นต่ำ (๑,๐๐๐ ครั้ง) ก็จะถือว่าเป็นโมฆะ และจะต้องเริ่มต้นการคลิกใหม่ในครั้งหน้า เพื่อสะสมจำนวนครั้งให้ได้ตามที่ระบุขั้นต่ำ เช่น หากคลิกได้เพียง ๗๘๐ ครั้ง แล้วมีเหตุจำเป็นที่จะต้องออกไปซื้อของข้างนอกบ้าน จำนวนคลิก ๗๘๐ ครั้งนี้ก็จะ**ไม่สามารถเปลี่ยนแปลงเป็นตัวเงินได้**

แต่ตรงนี้ จะต้องทำความเข้าใจว่า จำนวน ๗๘๐ ครั้งที่ไม่นับของผู้คลิกนั้น จะถูกนับรวมในนามของเอเย่นต์ ดังนั้น เอเย่นต์โฆษณาจะได้รับค่าตอบแทนจากผู้ผลิตตลอดเวลาที่มีผู้สนใจเข้ามาทดลองคลิกเพื่อหารายได้แต่ไม่ได้ตามจำนวนเป้าหมายขั้นต่ำ ซึ่งในทางปฏิบัติจริงแล้ว นอกจากขั้นต่ำ ๑,๐๐๐ ครั้งของการคลิกแล้ว ยังมีจำนวนยอดเงินสะสมขั้นต่ำที่จะต้องสะสมให้ได้ก่อนที่จะเบิกเงินได้อีก เช่น จะต้องคลิกเพื่อทำการสะสมยอดเงินรวมให้ได้ถึง ๒,๐๐๐ บาท เสียก่อน (เท่ากับต้องคลิก ๒๐๐,๐๐๐ ครั้ง) จึงจะสามารถเบิกเงินได้ ทำให้ในทางปฏิบัติแล้ว มีผู้คนเป็นจำนวนมากที่หลงเข้ามาทดลองหารายได้แล้วต้องล้มเลิกไป คำถามตรงจุดนี้คือ แล้วทำไมยังมีโฆษณา (ชวนเชื่อ) ให้คนไปทำงานประเภทนี้อยู่อีก (เอเย่นต์ต่างประเทศจะเสนอเงินเป็นสกุลดอลล่าร์ แต่เพื่อการเข้าใจง่ายจึงสมมุติเป็นเงินบาท)

คำตอบก็คือ ผู้ที่สนใจหารายได้ด้วยทำงานดังกล่าวสามารถหาตัวตายตัวแทน (หรือดาวน์ไลน์) ของตนเองเพื่อแบ่งยอดสะสมบางส่วนได้ ดังนั้น ผู้ที่หลงเข้ามาในวังวนนี้จึงพยายามเสาะหาตัวแทนที่จะมาคลิก แล้วตัวเองได้รับส่วนแบ่ง (ตามอัตราหรือ % ที่กำหนด) เพื่อว่าจะสามารถแปลงเป็นรายได้ โดยที่ตัวเองไม่ต้องลงแรงเอง ซึ่งมีหลายแหล่งข้อมูลเตือนว่าอย่าไปหลงเชื่อกับภาพถ่ายของเช็คหรือยอดเงินในสมุดบัญชีธนาคารที่แสดงว่าทำงานประเภทนี้แล้วได้เงินจริงๆ โดยเด็ดขาด เพราะนั่นคือกับดักที่จะทำให้หลงเข้าไปได้ (ไม่สามารถพิสูจน์ได้จริง)

๒) การแอบแฝงการทำธุรกรรมแบบลูกโซ่

มีข้อมูลเป็นจำนวนมากที่รายงานถึงพฤติกรรมการแอบแฝงการทำธุรกรรมแบบลูกโซ่ ผ่านการโฆษณาชวนเชื่อในลักษณะเช่นนี้ ซึ่งรูปแบบการโฆษณาแบ่งออกเป็น ๒ แบบ คือ ๑) ลงโฆษณาโดยให้ติดต่อกลับที่หมายเลขโทรศัพท์หรืออีเมลของตัวเองเพื่อสมัครเข้าทำงาน และ ๒) ลงโฆษณาโดยให้ติดต่อกลับไปยังหมายเลขโทรศัพท์หรืออีเมลของคนกลาง (หรือเบอร์กลาง)

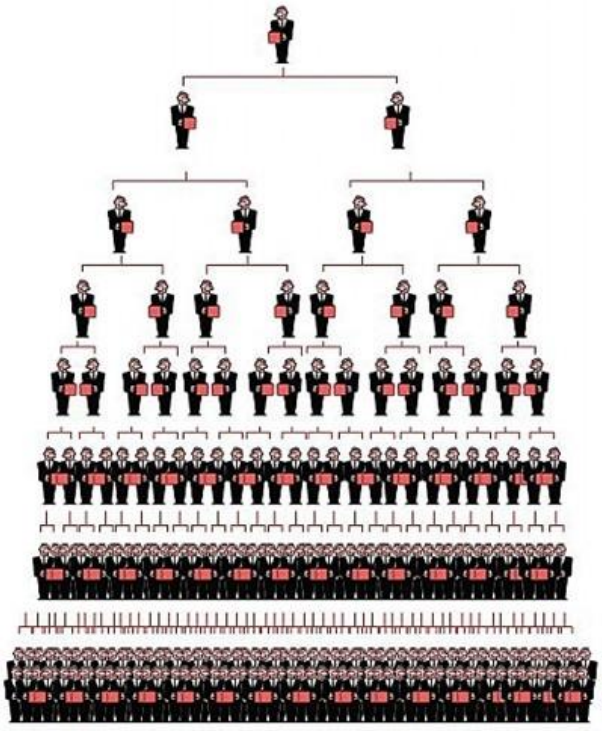
เพื่อสมัครเข้าทำงาน ซึ่งในรูปแบบที่ ๑ นั้น ผู้ที่สนใจสมัครจะได้พูดคุยโดยตรงกับผู้ลงโฆษณาเพื่อนัดวันเวลาสะดวกที่จะพบและพูดคุยกันถึงรายละเอียด ส่วนในรูปแบบที่ ๒ นั้น ผู้ที่สนใจสมัครจะได้พูดคุยกับคนกลางเพื่อนัดวันเวลาสะดวกที่จะพบและพูดคุยกันถึงรายละเอียด โดยในรูปแบบที่ ๒ นี้ ผู้สนใจสมัครงานจะต้องแจ้ง “รหัส” ประจำโฆษณานั้นๆ ด้วย เช่น หากในหน้าโฆษณาที่ดูมีการระบุถึงรหัส S.56094 เวลาที่ทำการสมัครก็จะต้องแจ้งรหัสดังกล่าวให้ผู้รับสมัครซึ่งเป็นคนกลางทราบด้วย และรหัสที่ว่านี้เองที่เป็นกุญแจดอกสำคัญในการเข้าถึงรูปแบบการปฏิบัติที่แท้จริงได้ในภายหลัง

หลังจากที่มีการพูดคุยกันในเบื้องต้นแล้ว (ทั้ง ๒ รูปแบบ) ผู้รับสมัครจะนัดวันเวลาและสถานที่ที่จะให้ไปพบกันเพื่อพูดคุยถึงรายละเอียดของงาน ตรงนี้ โดยส่วนใหญ่จะมีการกำหนดรอบของการจัดการพบปะเพื่อการอธิบายถึงรายละเอียด ให้กับผู้ที่สนใจจะสมัครพร้อมกันหลายๆ คน (บางครั้งอาจจะเป็นแบบผู้สมัครคนเดียวก็ได้) ซึ่งสถานที่มักจะเป็นที่ห้องจัดอบรมสัมมนาต่างๆ ของโรงแรมในย่านธุรกิจ ซึ่งเมื่อการพบปะดังกล่าวเริ่มขึ้น ผู้สมัครทุกคนก็จะถูกเชิญชวนให้สมัครเข้าร่วมเป็นสมาชิกก่อนโดยมีค่าใช้จ่ายเริ่มต้นจำนวนหนึ่ง และจะมีทีมงานมาบรรยายถึงข้อดีต่างๆ ของงาน พร้อมทั้งแสดงสูตรคำนวณรายได้ พร้อมพูดจาโน้มน้าวต่างๆ นาๆ ในหลายกรณี จะมีผลิตภัณฑ์ต่างๆ ในเครือมาเสนอมอบให้เป็นของรางวัลหรือสินค้าตอบแทน ประเด็นอยู่ที่ตรงนี้ครับ... เมื่อเราจ่ายเงินเพื่อสมัครงาน ผู้ที่แนะนำเราเข้าไป (หากเป็นแบบผ่านคนกลาง จะสามารถทราบตัวผู้ที่แนะนำเราได้จากรหัส เช่น S.56094 (ภาพที่ ๑.๒๒)) ก็จะได้รับเงินจำนวนนั้นไปบางส่วนหรือทั้งหมดเป็นค่าตอบแทน ซึ่งหากเราทำในลักษณะเดียวกัน คือ แนะนำให้คนอื่นมาร่วมสมัครเข้าเป็นสมาชิก เราก็จะได้ส่วนแบ่งจำนวนหนึ่งจากเงินก้อนนั้น และยิ่งเราหาสมาชิกใหม่เข้ามาเพิ่มได้มากเท่าไร เราก็มีโอกาสที่จะได้ส่วนแบ่งมากขึ้นเท่านั้น (โดยรวมแล้ว มีโอกาสได้เงินมากกว่าจำนวนที่เราเสียไปเป็นค่าสมัครในตอนแรก) หรือพูดง่ายๆ ก็คือรายได้ของเรา ก็มาจากค่าสมัครของคนที่เราแนะนำได้นั่นเอง และจะวนเวียนในลักษณะเดียวกันนี้เป็นทอดๆ ต่อไป

ภาพที่ ๑.๒๒ ตัวอย่างรหัสผู้แนะนำการทำงานผ่านอินเทอร์เน็ต

ยกตัวอย่างเช่น หากเราเสียเงินค่าสมัครสมาชิกก้อนแรกเป็นจำนวน ๕,๐๐๐ บาท เงินจำนวนนี้จะถูกแบ่งให้ผู้ที่แนะนำเรา ๕๐ % นั่นคือ ผู้ที่แนะนำเราไปจะได้ส่วนแบ่ง ๒,๕๐๐ บาท และอีก ๒,๕๐๐ บาทจะเป็นของทีมงานกลาง เช่นเดียวกัน หากเราสามารถแนะนำให้คนอื่นมาสมัครเป็นสมาชิกได้ เราก็จะได้ส่วนแบ่งเป็นจำนวนเงิน ๒,๕๐๐ บาทต่อสมาชิกใหม่ ๑ คน ด้วย ซึ่งหมายถึงหากเราหาสมาชิกมาเพิ่มได้มากกว่า ๒ คน เราก็จะมีกำไรถึง ๒,๕๐๐ บาทต่อคน

(ตั้งแต่ลำดับที่ ๓ เป็นต้นไป) นอกจากนี้ หากคนที่เราแนะนำเข้ามา (หรือดาวน์ไลน์ของเรา) สามารถหาสมาชิกใหม่เพิ่มได้อีก เราก็จะได้รับส่วนแบ่งเป็นเงินจำนวนหนึ่ง (เป็น %) จากเงินค่าแรกเข้าจำนวน ๕,๐๐๐ บาท ของสมาชิกใหม่คนนั้นด้วย โดยจะมีการกำหนดระดับชั้น (Layers) สูงสุดของดาวน์ไลน์เอาไว้ และจะสืบทอดในลักษณะเช่นนี้เรื่อยไปจนกว่าจะไม่มีผู้ที่หลงเชื่อเพิ่มเข้ามาในระบบอีก ทีมงานกลางนี้ก็จะสลายตัวไป เพื่อหาช่องทางในการหาเงินใหม่ ซึ่งจะเห็นว่าไม่แตกต่างอะไรกับระบบ MLM (Multi-Level Marketing) หรือการตลาดแบบลูกโซ่ (ภาพที่ ๑.๒๓)



ภาพที่ ๑.๒๓ Model การตลาดแบบลูกโซ่

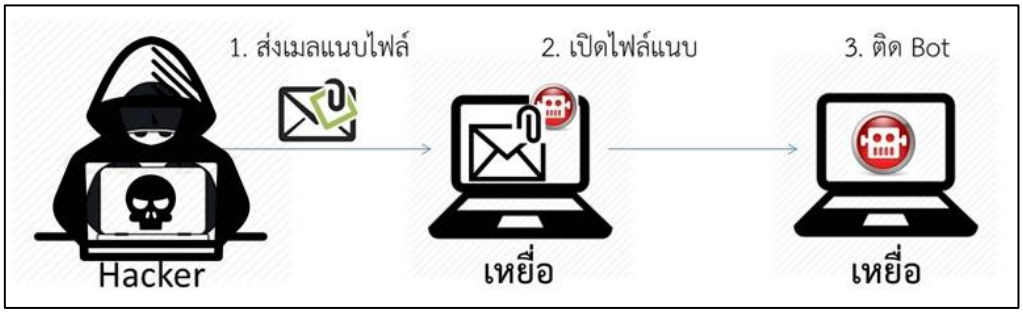
สิ่งที่เป็นการทำงานด้วยการคลิกผ่านเน็ตก็คือ การผนวกธุรกรรมลูกโซ่แบบดั้งเดิมเข้ากับระบบอินเทอร์เน็ตซึ่งเป็นระบบที่ใช้ในการติดต่อสื่อสารข้อมูลที่ทรงพลังอย่างยิ่งในปัจจุบัน ด้วยการเข้าไปไลโพสต์โฆษณาเชิญชวน (ชวนเชื่อ) ในลักษณะเดียวกัน ลงไปในช่องทางต่างๆ บนอินเทอร์เน็ต ซึ่งวิธีที่สะดวก ง่าย และรวดเร็วในการแนะนำคนอื่นก็คือ การส่งอีเมล (ในหลายกรณีทีมงานกลางจะมีกลุ่มรายชื่ออีเมลเตรียมไว้ให้) การโพสต์ลงตามบอร์ด และการโพสต์ลงในหน้า Facebook แล้ว Tag ชื่อของคนที่เป็นเพื่อนของเราเข้าไปมากๆ (โฆษณานั้นก็จะไปปรากฏบนหน้า Facebook ของคนนั้น ซึ่งเพื่อนๆ ของคนนั้นก็จะสามารถดูได้) โดยมีเนื้อหาการโฆษณาเชิญชวนตามตัวอย่างด้านบน และเมื่อมีคน (เหยื่อ) สนใจติดต่อมา ก็จะนัดให้ไปยังที่รับสมัคร สุดท้ายจะเข้าล็อคตามรูปแบบทุกประการ

ในกรณีที่มีระบบขายตรงเข้ามาปะปนด้วย ผู้สมัครจะได้รับการแนะนำให้หาเงินค่าสมัครเข้าเป็นสมาชิกด้วยการขายสินค้าขายตรงต่างๆ นั้น ให้กับกลุ่มเพื่อนของตนเอง เพื่อจะได้นำส่วนแบ่งรายได้มาเป็นค่าสมัคร และในกรณีที่ร้ายแรงกว่านั้นก็คือ ผู้สมัครจะต้องจ่ายเงินสด

เป็นค่าสมัคร โดยจะมีรายได้คืนกลับมาเป็นกำไรด้วยวิธีการขายสินค้าตรงนั้นๆ หรือการหาสมาชิกใหม่มาเพิ่มดังกล่าวข้างต้น ซึ่งมีผู้หลงเชื่อจำนวนไม่น้อยที่ไม่สามารถปฏิเสธการชักชวนอันแยบยลนั้นได้ หลายแหล่งข้อมูลบ่งบอกว่าปฏิบัติการโน้มน้าวและชักชวนนั้นกระทำเป็นทีมงาน เน้นไปที่การสร้างแรงบันดาลใจให้เกิดขึ้น โดยมีการแนะนำตัวอย่างของผู้ที่ประสบความสำเร็จได้เงินล้านภายในเวลาอันสั้น หรือแม้กระทั่งในหลายต่อหลายครั้ง ที่มีการนำรถสปอร์ตหรูราคาแพงจำนวนหลายคันมาจอดไว้หน้าบริเวณที่มีการนัดแนะพูดคุยถึงรายละเอียดของงาน เพื่อสร้างความน่าเชื่อถือและสร้างภาพแห่งความมั่งคั่งของผู้ที่เข้าร่วมทำงานในกลุ่มให้เกิดขึ้น

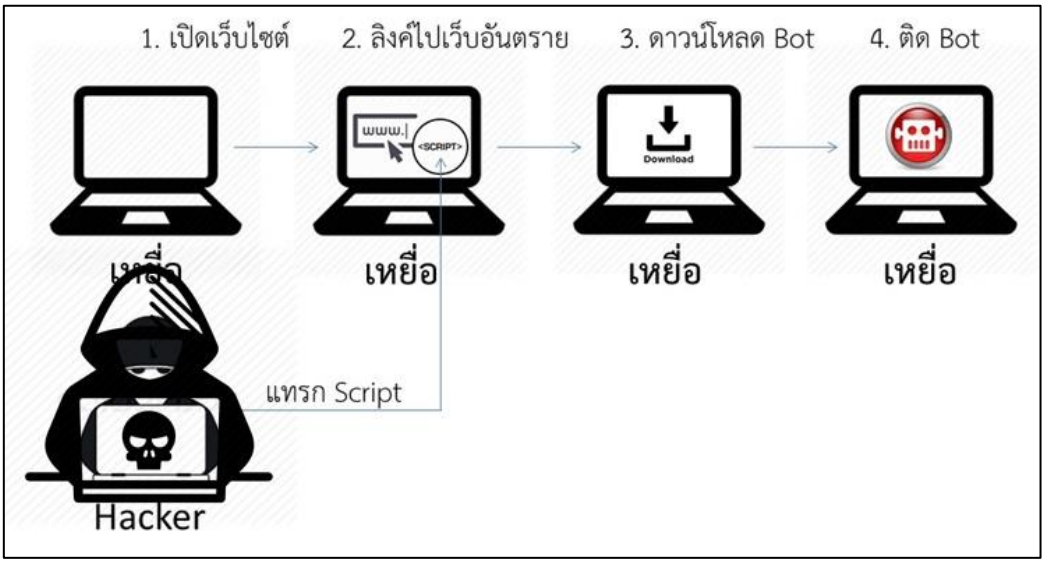
๑.๓.๘ บ็อทเน็ท (Botnet) เป็นชื่อของรูปแบบของมัลแวร์ชนิดหนึ่ง ซึ่งเมื่ออุปกรณ์คอมพิวเตอร์ติดมัลแวร์ชนิดนี้เข้าไป จะกลายเป็นอุปกรณ์ที่สามารถถูกสั่งการให้ปฏิบัติการทางไซเบอร์จากผู้เข้าควบคุมที่เชื่อมต่อมาจากระยะไกลได้ เปรียบเสมือนว่าอุปกรณ์คอมพิวเตอร์ที่ติดมัลแวร์นั้นทำหน้าที่เสมือนหุ่นยนต์ (roBOT) ซึ่งถูกบังคับจากระยะไกล โดยกลุ่มของอุปกรณ์คอมพิวเตอร์ที่ติดมัลแวร์ประเภทเดียวกันนี้ จะถูกบังคับควบคุมในลักษณะของเครือข่าย (NETwork) ให้ปฏิบัติการหรือร่วมปฏิบัติการใดๆ ทางไซเบอร์ ดังนั้น BOTNET จึงหมายถึง กลุ่มเครือข่ายของอุปกรณ์คอมพิวเตอร์ที่ติดมัลแวร์ชนิดนี้ ทำให้กลายเป็นเครือข่ายหรือฐานการปฏิบัติการร่วมของผู้ไม่ประสงค์ดีที่สามารถควบคุมใช้งานได้จากระยะไกล สำหรับอุปกรณ์คอมพิวเตอร์ที่ติดมัลแวร์ชนิดนี้ จะเรียกว่า BOTs หรือบางครั้งจะเรียกว่า Zombies มัลแวร์ประเภทนี้สามารถเข้าสู่อุปกรณ์คอมพิวเตอร์ที่ใช้งานได้ในหลากหลายรูปแบบ ดังนี้

๑.๓.๘.๑ อุปกรณ์คอมพิวเตอร์ (PC & Notebook Computer) รูปแบบนี้ BOT จะแฝงตัวมากับไฟล์แนบทางอีเมล (Mail Attachment File) เช่น อยู่ในลักษณะของไฟล์บีบอัด (.zip, .rar) โดยผู้ไม่ประสงค์ดีจะเป็นผู้สร้าง BOT ในลักษณะนี้ขึ้น แล้วหาช่องทางในการกระจายตัวของ BOT ผ่านไฟล์แนบส่งทางอีเมลไปยังกลุ่มเป้าหมาย (Target) โดยส่วนใหญ่จะสร้างเนื้อหาของอีเมลที่สามารถที่จะชักจูงให้ผู้รับมีความสนใจเพื่อหลอกให้ทำการคลิกเพื่อเปิดไฟล์แนบ เช่น เป็นเนื้อหาเกี่ยวกับสถาบันการเงินที่น่าจะมีความเกี่ยวข้องกับกลุ่มเป้าหมาย หรือเป็นเนื้อหาเกี่ยวกับการแจ้งเตือนจากผู้ให้บริการต่างๆ ทางอินเตอร์เน็ทแล้วร้องขอให้ผู้ใช้งานคลิกเปิดไฟล์แนบเพื่อตรวจสอบความถูกต้อง ฯลฯ ทั้งนี้ เมื่อกลุ่มเป้าหมายคนใดหลงเชื่อ ทำการคลิกเพื่อเปิดไฟล์ที่แนบมา BOT ก็จะทำงานโดยฝังตัวเองลงในเครื่องคอมพิวเตอร์นั้นทันที และเครื่องคอมพิวเตอร์นั้นก็จะกลายเป็นเหยื่อที่รวมเข้ากันกับกลุ่มเหยื่ออื่นๆ ในลักษณะของเครือข่ายคอมพิวเตอร์ที่ติด BOT (BOTNET) ซึ่ง Hacker สามารถที่จะเข้าควบคุมและสั่งการให้ปฏิบัติการต่างๆ ตามที่ต้องการได้จากระยะไกล (ภาพที่ ๑.๒๔)



ภาพที่ ๑.๒๔ การติด BOT ของอุปกรณ์คอมพิวเตอร์จากไฟล์แนบอีเมล

นอกจากนี้ BOT ยังสามารถแฝงตัวมากับหน้าเว็บไซต์ต่างๆ เช่น ในลักษณะของลิงค์ปลอม หรือ Pop-up โฆษณา (ภาพ/ข้อความ) ซึ่งจูงใจให้ผู้ใช้ทำการคลิกเพื่อเปิดดู (เช่น มีการแจกของรางวัล การแจกฟรี การมอบส่วนลดราคา ฯลฯ) โดยถูกตั้งให้เชื่อมต่อไปยังการดาวน์โหลดมัลแวร์ประเภท BOT หรือในลักษณะของการแทรกสคริปต์ (Script) บางอย่างเพิ่มลงในโค้ดของหน้าเว็บไซต์ ทำให้ถูกลิงค์ไปยังการดาวน์โหลด BOT โดยผู้ไม่ประสงค์ดีจะเป็นผู้แทรกช่องทางการนำไปสู่ลิงค์ปลอมที่จะเรียกดาวน์โหลดมัลแวร์ BOT ในลักษณะนี้ขึ้น แล้วรอให้กลุ่มเป้าหมาย (Target) มาติดกับดักและกลายเป็นเหยื่อด้วยการคลิกและดาวน์โหลด BOT ลงในเครื่องคอมพิวเตอร์ (ภาพที่ ๑.๒๕)



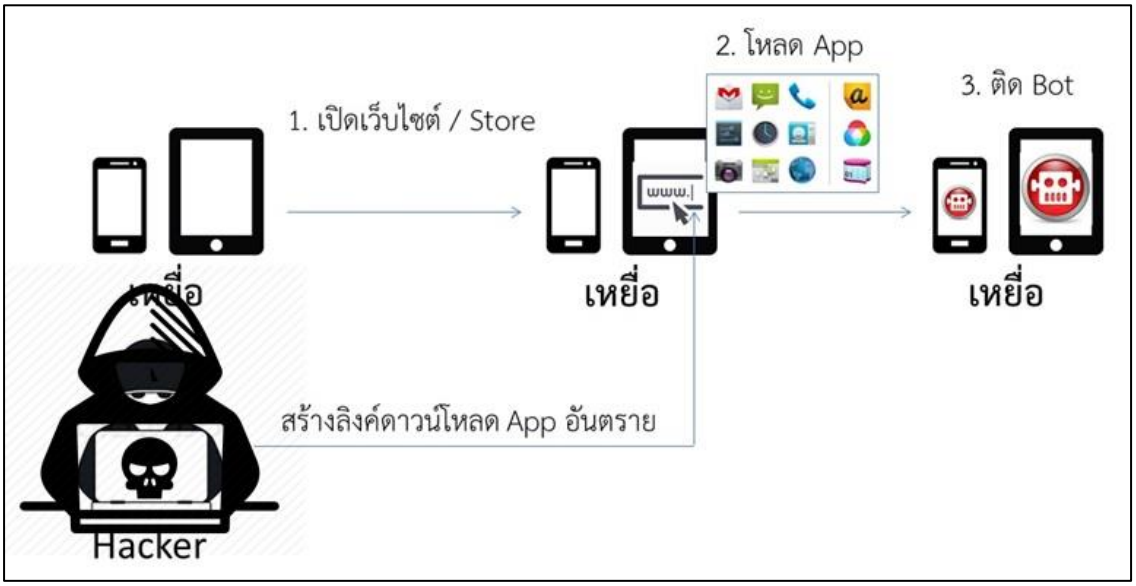
ภาพที่ ๑.๒๕ การติด BOT ของอุปกรณ์คอมพิวเตอร์จากการเปิดหน้าเว็บไซต์อันตราย

๑.๓.๘.๒ อุปกรณ์ Mobile Devices (Smart Phone & Tablet) รูปแบบนี้ BOT จะแฝงตัวมากับแหล่งดาวน์โหลดแอพพลิเคชั่น (Application) ที่อยู่บนหน้าเว็บไซต์หรือใน Store ต่างๆ เช่น ในลักษณะของลิงค์ปลอม หรือ Pop-up โฆษณา (ภาพ/ข้อความ) หรือไอคอนของแอพพลิเคชั่นที่ถูกตั้งให้เชื่อมต่อไปยังการดาวน์โหลดแอพพลิเคชั่นที่พ่วงมัลแวร์ประเภท BOT เข้าไปด้วย โดยผู้ใช้จะสามารถเรียกใช้งานแอพพลิเคชั่นนั้นๆ ได้ตามปกติ แต่ BOT จะถูกฝังลงในอุปกรณ์สื่อสารแบบพกพา (Smart Phone, Tablet) ที่ใช้ (ภาพที่ ๑.๒๖)

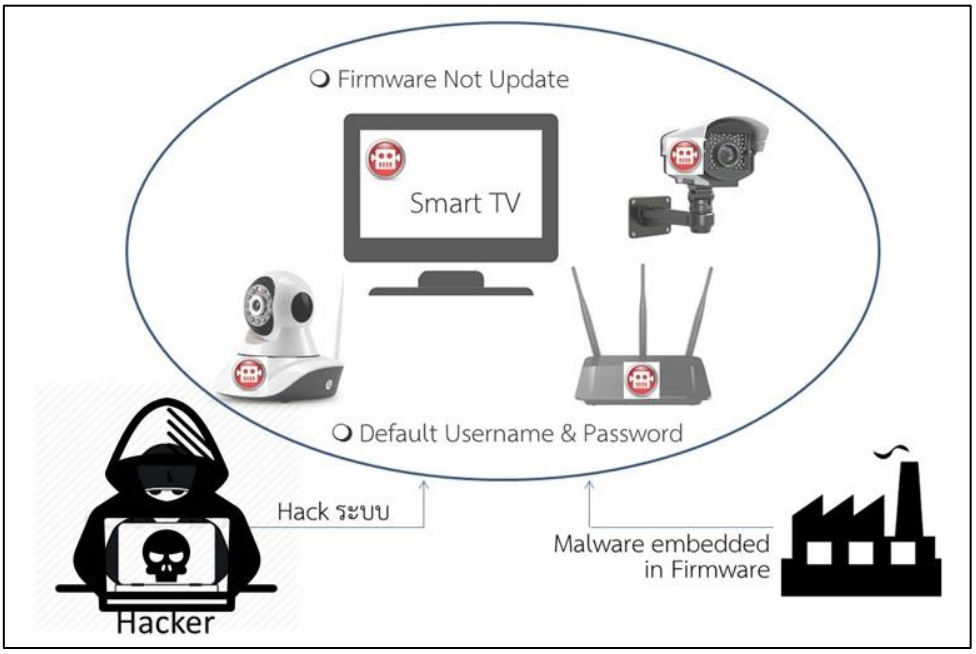
๑.๓.๘.๓ อุปกรณ์ Internet of Things: IoT (IP Camera, CCTV, Home Router, Smart TV) รูปแบบนี้ BOT จะแฝงตัวมาใน Firmware ของอุปกรณ์ Internet of Things (IoT) บางประเภทที่ผู้ผลิตหรือผู้จัดจำหน่าย/ผู้จัดส่ง สามารถเข้าถึงและเปลี่ยนแปลงซอฟต์แวร์บางส่วนใน Firmware เองได้ โดยตั้งใจที่จะใช้เป็นช่องทางสำหรับการสำรวจหรือตรวจสอบข้อมูลบางอย่างของการทำงานของตัวอุปกรณ์ รวมทั้งการบำรุงรักษาอุปกรณ์ด้วยการเชื่อมต่อจากระยะไกลด้วยชื่อผู้ใช้งานกับรหัสผ่านระดับผู้ควบคุมอุปกรณ์ (Administrator) ที่ถูกโปรแกรมเตรียมเอาไว้แล้ว ซึ่งตรงนี้เองเป็นช่องโหว่ที่ทำให้ผู้ไม่ประสงค์ดีสามารถใช้เป็นช่องทางในการนำพามาซึ่ง BOT ในตัวอุปกรณ์

ได้ ทั้งนี้ รวมถึงอุปกรณ์ IoT อื่นๆ เช่น CCTV, IP Camera, Home Router ฯลฯ ที่ผู้ใช้ไม่ทำการเปลี่ยนชื่อผู้ใช้งานและรหัสผ่านที่ตั้งมาจากโรงงาน (Factory Default Username & Password) ให้เป็นค่าใหม่ซึ่งตั้งโดยผู้ใช้งานเอง ก็สามารถติด BOT ได้ด้วยลักษณะการนำเข้า BOT แบบที่ Hacker เชื่อมต่อเข้ามาที่อุปกรณ์จากระยะไกลโดยใช้ชื่อผู้ใช้และรหัสผ่านเดิมจากโรงงานนั้น พบว่าข้อมูลเหล่านี้สืบค้นได้จากทางอินเทอร์เน็ตทั่วไปได้โดยง่าย เช่น CCTV ยี่ห้อ AVTECH บางรุ่นที่รองรับการเชื่อมต่อทางอินเทอร์เน็ต จะใช้ชื่อผู้ใช้/รหัสผ่าน เป็น “admin/admin” ถูกระบุโดย SHODAN ซึ่งเป็น Search Engine ด้าน Security ว่าปัจจุบันพบว่ามีผู้เชื่อมต่อกล้อง CCTV นี้เข้ากับระบบอินเทอร์เน็ตโดยใช้ชื่อผู้ใช้งาน/รหัสผ่านเดิมที่ตั้งมาจากโรงงานเป็นจำนวนมาก (ใครก็สามารถเรียกดูได้จากอินเทอร์เน็ตเช่นกัน) ทำให้การเพิ่มจำนวนของ BOTNET ในอุปกรณ์ประเภท Internet of Things (IoT) นี้เพิ่มขึ้นเป็นจำนวนมากในห้วงเวลาที่ผ่านมา (ภาพที่ ๑.๒๗)

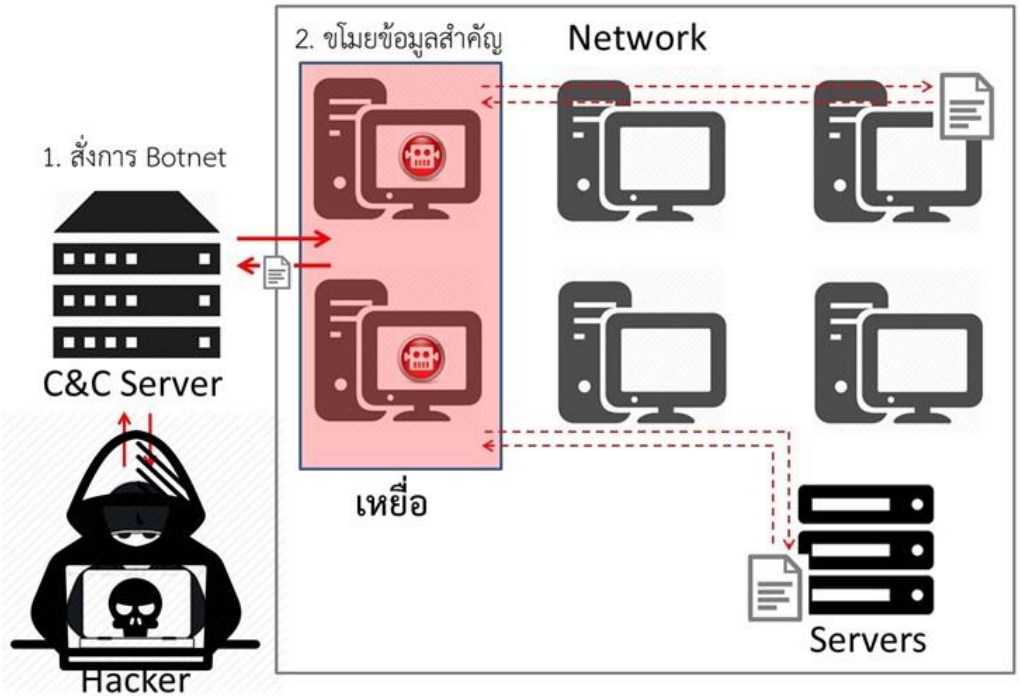
เครื่องที่ติด BOT และอยู่ในเครือข่าย BOTNET จะสามารถถูกควบคุมโดย Hacker จากระยะไกลได้ โดย Hacker จะทำการสั่งการและควบคุม BOTNET ผ่านเครื่องแม่ข่ายในการสั่งการและควบคุมที่เรียกว่า “Command & Control Server: C&C Server” ในลักษณะที่อาจจะใช้ BOTNET เป็นฐานในการขโมยหรือให้ได้มาซึ่งข้อมูลสำคัญจากหน่วยงานเป้าหมาย (ภาพที่ ๑.๒๘) หรือใช้ BOTNET เป็นฐานในการโจมตีทางไซเบอร์ต่อเป้าหมาย (ภาพที่ ๑.๒๙) เช่น การระดมโจมตีเพื่อให้เครื่องแม่ข่ายเป้าหมายหยุดทำงาน (Distributed Denial of Service: DDoS) การระดมส่งสแปมเมลไปยังผู้รับซึ่งอยู่ในบัญชีติดต่อของเครื่อง BOTNET ทั้งนี้ ปฏิบัติการต่างๆ ทั้งหมดจะเกิดจากเครื่อง BOTNET ไปยังเป้าหมาย โดยผู้ใช้งานอุปกรณ์คอมพิวเตอร์ที่เป็น BOTNET ไม่รู้ตัว



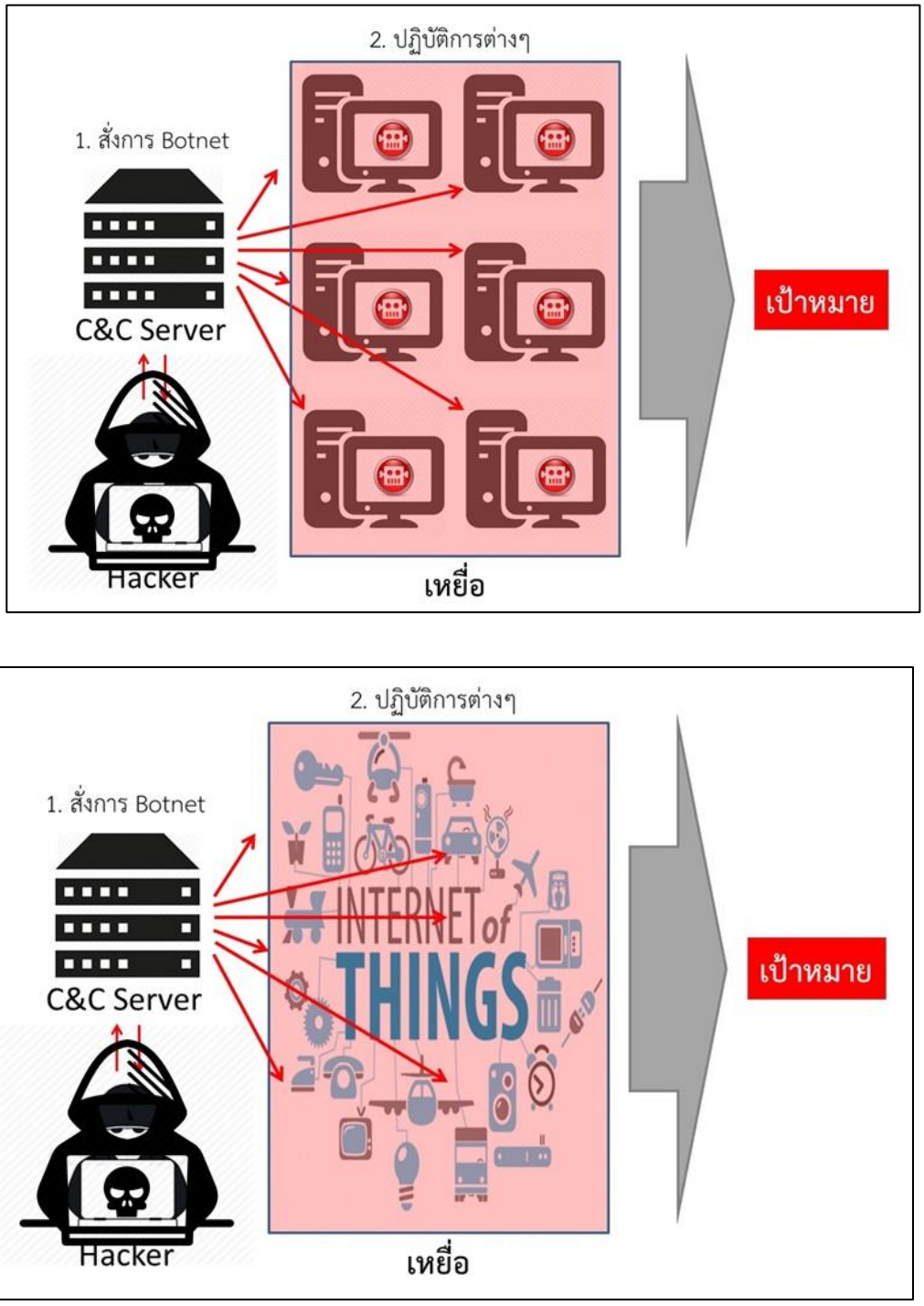
ภาพที่ ๑.๒๖ การติด BOT ของอุปกรณ์ Mobile Devices จากการเปิดหน้าเว็บไซต์ / Store อันตราย



ภาพที่ ๑.๒๗ การติด BOT ของอุปกรณ์ IoT จาก Firmware หรือการถูกแฮก



ภาพที่ ๑.๒๘ เครื่องที่ติด BOT ถูกใช้ในการขโมยข้อมูลสำคัญจากหน่วยงานเป้าหมาย



ภาพที่ ๑.๒๙ เครื่องที่ติด BOT ถูกใช้ในการโจมตีต่อเป้าหมาย

แนวทางการป้องกันบ็อทเน็ท (Botnet) สามารถปฏิบัติได้ ดังนี้

๑) ไม่เปิดอีเมล/ไฟล์แนบ/ลิงค์ ที่มาจากแหล่งที่ไม่รู้จัก หรือรู้จักแต่ผิดปกติวิสัย

๒) ไม่เปิด หรือดาวน์โหลดไฟล์ จากเว็บไซต์ที่อันตราย หรือน่าสงสัย หรือไม่น่าเชื่อถือ โดยเฉพาะเว็บไซตประเภทโฆษณา/แจกของ/ลดราคา/ฟรีแวร์

3) ไม่เจลเบรค (Jail Break) อุปกรณ์สื่อสารแบบพกพาที่ใช้งาน

๔) ติดตั้งซอฟต์แวร์ป้องกันไวรัส และทำการอัพเดทส่วนของ Engine และฐานข้อมูลไวรัส ให้เป็นปัจจุบันเสมอ

๕) อัพเดทระบบปฏิบัติการคอมพิวเตอร์ (Operating System: OS) ให้เป็นปัจจุบันเสมอ

๖) เปิดใช้งานไฟล์วอล (Firewall) ของเครื่องคอมพิวเตอร์

๗) เปลี่ยนรหัสผ่านอุปกรณ์คอมพิวเตอร์และเครือข่าย ตลอดจนอุปกรณ์ IoT ที่ตั้งมาจากโรงงาน (Default Password) เป็นรหัสผ่านใหม่เสมอ

๑.๓.๙ การแฮก (Hacking) เป็นรูปแบบการโจมตีแบบเฉพาะเจาะจงเป้าหมายที่ต้องการ (Targeted Attack) โดยผู้ไม่ประสงค์ดีหรือแฮกเกอร์ ด้วยกระบวนการและเครื่องมือทางไซเบอร์ การเข้าโจมตีเป้าหมายแบบเฉพาะเจาะจงนั้น เป็นรูปแบบหนึ่งของภัยคุกคามที่เรียกว่า APT (Advanced Persistent Threat) ที่มีเป้าหมายของการโจมตีเจาะจงไปที่หน่วยงานที่มีข้อมูลสำคัญเช่น หน่วยงานด้านความมั่นคงและการทหาร หน่วยงานด้านการเมืองการปกครอง ตลอดจนหน่วยงานทางภาคธุรกิจที่มีขนาดใหญ่ เช่น Google และ Amazon โดยแฮกเกอร์จะใช้วิธีการบุกรุกเข้าไปในระบบสารสนเทศของเป้าหมายด้วยการใช้เครื่องมือและเทคนิคที่หลากหลาย ตั้งแต่ใช้ศาสตร์ความรู้ชั้นสูงด้านคอมพิวเตอร์ในการเจาะเข้าระบบ จนถึงการใช้เทคนิคพื้นฐานด้านปฏิบัติการจิตวิทยาในการหลอกลวงหรือหลอกล่อบุคคลหรือกลุ่มบุคคลที่อยู่ในองค์กรที่เป็นเป้าหมายผ่านช่องทางเครือข่ายสังคมแบบออนไลน์ต่างๆ เพื่อให้เปิดเผยข้อมูลสำคัญอันเป็นประโยชน์ในการเจาะเข้าสู่ระบบขององค์กรเป้าหมาย หรือหลอกล่อให้ดาวน์โหลดโปรแกรมต่างๆ ที่ใช้ประโยชน์ในการเจาะระบบภายใต้ความไม่ระวังของผู้ใช้งาน เช่น หลอกให้เปิดไฟล์ที่แนบมากับอีเมล หรือหลอกให้เปิดเว็บไซต์ที่อันตราย หรือหลอกให้ติดตั้งโปรแกรมปลอมเป็นต้น เพื่อเจาะเข้าสู่ระบบและปฏิบัติการตามวัตถุประสงค์ที่ต้องการได้ในภายหลัง

ในทางปฏิบัติเชิงเทคนิค กระบวนการบุกรุก (Intrusion Process) แบ่งออกเป็น ๓ ขั้นตอนหลัก (๓ Stages) ที่สำคัญ ดังนี้

Stage ๑ : การเปิดช่องทางในการเชื่อมต่อเข้าสู่ระบบ (Code Execution)

ผู้ไม่ประสงค์ดีจะทำการลาดตระเวณในโลกไซเบอร์เพื่อค้นหา User เป้าหมาย หลังจากนั้นจะส่งอีเมล ฯลฯ ที่มีมัลแวร์หรือลิงค์ไปยังเว็บไซต์อันตรายแนบปะปนเข้าไปด้วย โดยการปฏิบัติการแบบวิศวกรรมสังคม (Social Engineering) เช่นนี้ ปฏิบัติได้ง่าย โดยเฉพาะหน่วยงานที่แสดงข้อมูลส่วนตัว (เช่น ชื่อ นามสกุล ตำแหน่ง) และอีเมล (Email Address) ของบุคลากรภายในไว้บนหน้าเว็บไซต์ของหน่วยงาน และจะง่ายยิ่งขึ้น หากบุคลากรในหน่วยงานมีการนำอีเมล (ของที่ทำงาน) ของตัวเองไปใช้กับเรื่องอื่นที่ไม่เกี่ยวกับเรื่องงานด้วย เนื่องจากว่าหัวข้อที่สามารถใช้ในการหลอกลวงจะกระทำได้ง่ายยิ่งขึ้น เช่น หัวข้อเกี่ยวกับการกู้ยืมเงิน หัวข้อเกี่ยวกับการซื้อสินค้าเป็นต้น โดยเมื่อผู้ใช้งานของหน่วยงานที่เป็นเป้าหมายดังกล่าวเปิดไฟล์แนบที่มากับอีเมลหรือคลิกเปิดลิงค์ไปยังเว็บไซต์อันตรายดังกล่าว Malicious Code จะฝังตัวเข้าสู่คอมพิวเตอร์ที่ใช้งานในทันที ซึ่งโดยปกติแล้ว Malicious Code ดังกล่าวจะตั้งให้เปิดขึ้นมาทุกครั้งที่มีการเปิดใช้งานเครื่องคอมพิวเตอร์ ซึ่งการเปิด (Execute) ของ Malicious Code นี่เอง ที่ทำให้ผู้ไม่ประสงค์ดีสามารถใช้เป็นช่องทางในการเข้าถึง (Access) เครื่องคอมพิวเตอร์นั้นๆ ได้

Stage ๒ : การขยายตัวเข้าไปในระบบเครือข่าย (Network Propagation)

ผู้ไม่ประสงค์ดีจะเคลื่อนตัวเข้าไปในระบบเครือข่ายภายในของหน่วยงาน เพื่อเข้าถึงข้อมูลที่ต้องการที่อยู่ในคอมพิวเตอร์หรือเครื่องแม่ข่ายอื่นในระบบ เช่น ข้อมูลไฟล์สำคัญ ข้อมูลผู้ใช้งาน ข้อมูลสิทธิ์ของผู้ใช้งาน ข้อมูลการตั้งค่าระบบเครือข่าย (Network Configurations) ตลอดจนข้อมูลรหัสผ่านของผู้ใช้งาน (User Passwords/Passphrases) เป็นต้น ทั้งนี้ ถึงแม้ว่าข้อมูลรหัสผ่านมักจะถูกเก็บไว้ในรูปของการทำ Cryptographic Hashing ก็ตาม การ Crack รหัสผ่านที่มีระดับความปลอดภัยที่ต่ำ เช่น ตั้งเป็นตัวเลขหรือมีความยาวน้อย ก็พบว่าสามารถปฏิบัติได้ในระยะเวลาอันสั้น

Stage ๓ : การดึงข้อมูลสำคัญที่ต้องการ (Data Exfiltration)

ผู้ไม่ประสงค์ดีทำการดึงข้อมูลสำคัญที่ต้องการจากระบบเครือข่ายผ่านทางเน็ตเวิร์คโปรโตคอล (Network Protocols) และพอร์ต (Port) ที่ได้รับอนุญาตภายในระบบเครือข่าย เช่น ผ่านทาง HTTPS/HTTP หรือ ทางช่องทาง DNS หรือ อีเมล เป็นต้น และโดยปกติแล้วผู้ไม่ประสงค์ดีจะยังคงรักษาช่องทางในการเข้าสู่ระบบ (Maintaining Access) ด้วยการสร้าง Backdoor ไว้สำหรับการย้อนกลับเข้ามาล้วงข้อมูลสำคัญอื่นๆ อีกในอนาคต

แนวทางการป้องกันการแฮก (Hacking) สามารถปฏิบัติได้ ดังนี้

๑) อัพเดทระบบปฏิบัติการคอมพิวเตอร์ (Operating System: OS) ให้เป็นปัจจุบันเสมอ

๒) บังคับใช้การตั้งค่ารหัสผ่านในระดับที่ปลอดภัย (Enforce a Strong Password Policy)

๓) บล็อคเว็บไซต์อันตราย (Web Blocking)

๔) เก็บข้อมูลการใช้งานระบบเครือข่าย (Network Activity Logging) และเฝ้าระวัง

๕) ติดตั้งไฟร์วอล (Firewall) / ระบบป้องกันการบุกรุก (IPS/IDS)

๖) ใช้การเข้ารหัสใน Transportation Layer (TLS)

๗) ใช้โปรแกรมป้องกันไวรัสและมัลแวร์และอัพเดทให้เป็นปัจจุบันเสมอ

๘) จัดแบ่งส่วนของเครือข่าย (Network Segmentation) ตามความสำคัญ

๙) ตั้งค่าต่างๆ (Configurations) ของอุปกรณ์เครือข่ายให้มีความปลอดภัย

๑๐) จัดทำ Blacklist ของ IP/Gateway อันตราย

๑๑) จัดแบ่งกลุ่มผู้ใช้ทรัพยากรสารสนเทศ พร้อมทั้งกำหนดสิทธิ์การเข้าถึง

๑๒) เพิ่มองค์ประกอบในการพิสูจน์ตัวตนเป็นแบบพหุปัจจัย (Multi-factor Authentication)

๑๓) จัดทำการตรวจประเมินความปลอดภัยภายใน (Penetration Testing) เพื่อแก้ไขปรับปรุง

๑๔) สร้างเสริมจิตสำนึกด้านความปลอดภัย (Security Awareness) แก่บุคลากรทุกระดับ

๑๕) ออกกฎ ระเบียบ หรือข้อปฏิบัติเพื่อความปลอดภัย และบังคับใช้กับบุคลากรทุกระดับ

๑.๓.๑๐ การทำวิศวกรรมสังคม (Social Engineering) คือ รูปแบบของการโจมตีทางไซเบอร์ที่ไม่ใช่การโจมตีแบบใช้เทคนิคเชิงเทคโนโลยีหรือใช้เครื่องมือประเภทเจาะระบบ โดยมุ่งเป้าไปที่ปฏิกิริยาตอบสนองของมนุษย์ปัจจัย (Human Interaction) เพื่อพยายามที่จะหลอกล่อเอาข้อมูลสำคัญอันเป็นประโยชน์ต่อการปฏิบัติการโจมตีทางไซเบอร์ (Cyber Attack) รวมทั้งการคาดหวัง

พฤติกรรมในเชิงละเมิดต่อกฎระเบียบทางด้านความปลอดภัยของบุคคลในองค์กร เพื่อเปิดช่องทางสู่การปฏิบัติการโจมตีให้กับผู้ไม่ประสงค์ดี

ปฏิบัติการ Social Engineering นั้น โดยพื้นฐานจะใช้วิธีการสร้างความสัมพันธ์กับบุคคลเป้าหมายทั้งแบบพบปะพูดคุยแบบเห็นหน้าและแบบสร้างความรู้จักผ่านสื่อสังคมออนไลน์ต่างๆ แล้วพยายามที่จะสร้างความคุ้นเคยสนิทสนม เพื่อขยายผลให้ได้มาซึ่งข้อมูลหรือข่าวสารที่ต้องการ อันจะเอื้อประโยชน์ต่อการปฏิบัติการโจมตีทางไซเบอร์ในอนาคต เช่น การขโมยข้อมูลเกี่ยวกับอัตลักษณ์ (Identity) ของบุคคล การหลอกถามชื่อผู้ใช้งานและรหัสผ่าน การสืบหาข้อมูลที่เกี่ยวข้อง เช่น พฤติกรรมในการเดินทาง พฤติกรรมในการทำงาน ยานพาหนะที่ใช้ วันเดือนปีเกิด กลุ่มเพื่อนฝูงที่มักมีปฏิสัมพันธ์ด้วย สถานที่ที่มักเดินทางไป ผู้บังคับบัญชาหรือหัวหน้างานที่ติดต่อด้วย กลุ่มลูกค้าที่ทำธุรกิจด้วย ช่องทางในการติดต่อสื่อสารกับบุคคลในองค์กร ธนาคารและบัตรเครดิตที่ใช้ ตลอดจนช่องทางในการสั่งซื้อสินค้าและชำระเงินแบบออนไลน์ เป็นต้น นอกจากนี้ ปฏิบัติการ Social Engineering ยังสามารถปฏิบัติได้แบบที่ไม่ต้องสร้างความสัมพันธ์หรือความสนิทสนมคุ้นเคยให้เกิดขึ้นก่อน แต่เป็นการหลอกล่อด้วยกลวิธีต่างๆ โดยใช้จุดอ่อนด้านการหลงเชื่อของมนุษย์ เพื่อให้ได้มาซึ่งข้อมูลที่ต้องการ เช่น การส่งอีเมลหลอกลวง และการส่งข้อความหลอกลวงทางสื่อสังคมออนไลน์ เป็นต้น

๑.๓.๑๐.๑ หลักการพื้นฐานทางมนุษยศาสตร์ จากการที่ Social Engineering มุ่งเป้าไปที่มนุษย์ปัจจัย ดังนั้นการปฏิบัติการทางวิศวกรรมสังคมจะใช้หลักการพื้นฐานทางมนุษยศาสตร์ในด้านต่างๆ เพื่อหลอกล่อเอาข้อมูลสำคัญที่ต้องการ อาทิเช่น

๑) การสร้างความรู้สึกขอบคุณหรือเกรงใจ ซึ่งผู้ปฏิบัติการจะพยายามทำความรู้จักต่อบุคคลเป้าหมายและสร้างความสนิทสนมคุ้นเคย โดยพยายามคอยหยิบยื่นความช่วยเหลือต่างๆให้เมื่อมีโอกาส ทำให้เป้าหมายเกิดความรู้สึกขอบคุณและเกรงใจขึ้น จึงมักยินดีที่จะพูดคุยหรือตอบคำถามบางอย่างให้แก่ผู้ปฏิบัติการ โดยไม่รู้ตัวว่าข้อมูลต่างๆ ที่ให้ไปนั้นอาจเป็นข้อมูลที่ผู้ปฏิบัติการสามารถนำไปขยายผลต่อยอดในการโจมตีทางไซเบอร์ได้ในอนาคต

๒) การสร้างความน่าเชื่อถือ ผู้ปฏิบัติการจะสร้างความน่าเชื่อถือของตัวเองให้เกิดขึ้นในสายตาของบุคคลเป้าหมาย เช่น การพูดคุยด้วยข้อมูลเชิงเทคนิค เพื่อแสดงตัวว่าเป็นผู้เชี่ยวชาญด้านคอมพิวเตอร์ สามารถที่จะให้ข้อแนะนำเกี่ยวกับปัญหาด้านการรักษาความปลอดภัยของระบบให้ได้ โดยเมื่อเป้าหมายรู้สึกว่าผู้ปฏิบัติการนั้นมีความน่าเชื่อถือ ก็อาจจะอธิบายถึงปัญหาที่เกิดขึ้นในระบบคอมพิวเตอร์และเครือข่าย พร้อมทั้งข้อมูลด้านอุปกรณ์ เครื่องมือ ตลอดจนระบบที่เกี่ยวข้อง เพื่อเป็นการขอคำปรึกษาจากผู้ปฏิบัติการ ทำให้ผู้ปฏิบัติการนั้นได้มาซึ่งข้อมูลทางเทคนิคในเชิงลึกได้โดยง่าย โดยปฏิบัติการภายใต้การสร้างความน่าเชื่อถือนี้ สามารถเกิดขึ้นได้แบบไม่ต้องสร้างความรู้จักหรือสนิทสนมคุ้นเคยก่อน เช่น การที่ผู้ไม่ประสงค์ดีโทรศัพท์เข้าไปยังฝ่ายดูแล IT ขององค์กร แล้วปลอมตัวว่าเป็นผู้บริหารระดับสูงขององค์กร พร้อมแจ้งปัญหาการไม่สามารถ Login เข้าสู่ระบบสารสนเทศต่างๆ ได้ และสอบถามข้อแนะนำด้านเทคนิค ทำให้สามารถที่จะได้มาซึ่งข้อมูลสำคัญที่เป็นประโยชน์ในการปฏิบัติการโจมตีทางไซเบอร์ได้

๓) การข่มขู่ ผู้ปฏิบัติการจะใช้วิธีการข่มขู่หรือบังคับบุคคลเป้าหมายด้วยวิธีต่างๆ เช่น การขู่ว่ามีภาพบางอย่างที่ไม่เหมาะสมของบุคคลเป้าหมายและจะโพสต์ภาพนั้นลงในสื่อสังคมออนไลน์ เพื่อให้ยินยอมมอบข้อมูลที่ต้องการให้ เพื่อเป็นการแลกเปลี่ยน ซึ่งปัจจุบัน ภาพ

ข้อความการพูดคุยทางแอพพลิเคชั่นสนทนาต่างๆ เช่น LINE, Facebook ที่ถูก Capture บางตอนซึ่งมีข้อความไม่เหมาะสมมา ก็สามารถใช้เป็นสิ่งขู่บังคับบุคคลเป้าหมายได้ โดยเฉพาะบุคคลเป้าหมายที่อยู่ในระดับสูงขององค์กรหรือสังคม

๔) ความอยากได้ ผู้ปฏิบัติการจะใช้วิธีหลอกล่อที่จะหยิบยื่นของรางวัลหรือสิ่งตอบแทนให้กับบุคคลเป้าหมาย เพื่อแลกกับการกระทำบางอย่าง เช่น หลอกล่อให้กรอกชื่อบัญชีอีเมล หรือข้อมูลอื่นๆ ที่เกี่ยวกับข้อมูลส่วนบุคคล หรือเกี่ยวกับเรื่องงาน ภายใต้ข้อเสนอที่มีสิทธิ์ในการรับรางวัลต่างๆ เป็นต้น ซึ่งในปัจจุบันนั้น พบว่า การโพสต์ข้อความเชิญชวนให้ทุกคนเขียนรหัสผ่าน (Password) ของตัวเองที่ใช้งานมาแลกเปลี่ยนกันดูเพื่อความสนุกสนาน โดยไม่ต้องบอกชื่อนามสกุลจริงใดๆ และไม่ต้องบอกชื่อบัญชีผู้ใช้งาน (Username) และจะมีการสุ่มมอบรางวัลบางอย่างให้กับผู้เข้าร่วมสนุก มีผลทำให้มีผู้หลงเชื่อมากรอกรหัสผ่านของตัวเองลงเป็นจำนวนมาก พร้อมกับความสนุกสนานในการ Comment เกี่ยวกับ Password บางตัวของผู้อื่น ซึ่งตรงนี้นับว่าอันตรายเป็นอย่างยิ่ง เนื่องจากชื่อบัญชีผู้ใช้งาน (Username) นั้น สามารถสืบค้นได้โดยง่ายด้วยเครื่องมือ Search Engine ทางอินเทอร์เน็ต และสิ่งที่น่ากลัวกว่านั้นก็คือ ข้อเท็จจริงที่ว่า บุคคลมักใช้รหัสผ่านเดียวกันกับหลายๆบัญชีการให้บริการ (อีเมลส่วนตัว, อีเมลที่ทำงาน, Mobile Banking) ทำให้ผู้ปฏิบัติการสามารถสืบค้นหาข้อมูลสำคัญและขยายผลสู่ระบบสารสนเทศขององค์กรหรือระบบการเงินการธนาคารอื่นได้โดยง่าย

๕) ความละเลย/ไม่ใส่ใจ ผู้ปฏิบัติการจะใช้ประโยชน์จากความละเลยหรือไม่ใส่ใจในการปฏิบัติของมนุษย์ปัจจัย โดยเฉพาะความละเลยต่อระเบียบขั้นตอนในการรักษาความปลอดภัย เพราะบุคคลหนึ่งบุคคลใด มักไม่คิดว่าตัวเองหรือองค์กรจะตกเป็นเป้าหมายในการโจมตี และจากผลการประเมินความตระหนักทางด้านความปลอดภัยทางไซเบอร์ พบว่า ประเทศไทยเป็นหนึ่งในกลุ่มประเทศที่นับว่าประชาชนมีความตระหนักเกี่ยวกับการรักษาความปลอดภัยและภัยคุกคามทางไซเบอร์ในระดับไม่สูง ทำให้การรักษาความปลอดภัยที่มักจะสวนทางกับความสะดวกสบาย ไม่ได้รับการปฏิบัติอย่างเคร่งครัดจริงจัง จึงอาจก่อให้เกิดเป็นช่องโหว่สำคัญของการโจมตีได้ หนึ่งในตัวอย่างที่ใกล้ตัว ได้แก่ การที่องค์กรมีกฎระเบียบในการตั้งค่ารหัสผ่านและระยะเวลาหรือวงรอบในการเปลี่ยนรหัสผ่าน แต่ในทางปฏิบัติจริง พบว่ามีผู้ที่ปฏิบัติตามเป็นจำนวนที่น้อยมาก มีคำกล่าวที่ว่า ระบบซอฟต์แวร์ต่างๆ สามารถแก้ไขหรือปิดช่องโหว่ได้จากการปรับปรุงซอฟต์แวร์ให้มีความทันสมัย (Patching) แต่มนุษย์ปัจจัยไม่มีการทำ Patching ที่สามารถแก้ไขหรือปิดช่องโหว่ได้โดยอัตโนมัติด้วยการอัพเดทใดๆ นอกเหนือจากการให้ความรู้เกี่ยวกับภัยคุกคามและอันตรายที่อาจจะเกิดขึ้นเพื่อสร้างความตระหนักในภัยอันตรายทางไซเบอร์ และต้องมีการให้ความรู้อยู่เสมอเพื่อให้เท่าทันต่อความเปลี่ยนแปลงของเทคโนโลยีและภัยคุกคามทางไซเบอร์ที่มีการพัฒนาตัวในทุกขณะ

๑.๓.๑๐.๒ ขั้นตอนการปฏิบัติการ Social Engineering เช่นเดียวกับหลักการโจมตีทางไซเบอร์ (Cyber Attack) ประเภทอื่น Social Engineering มีขั้นตอนในการปฏิบัติการหลัก ๔ ขั้นตอน (ภาพที่ ๑.๓๐) ดังนี้

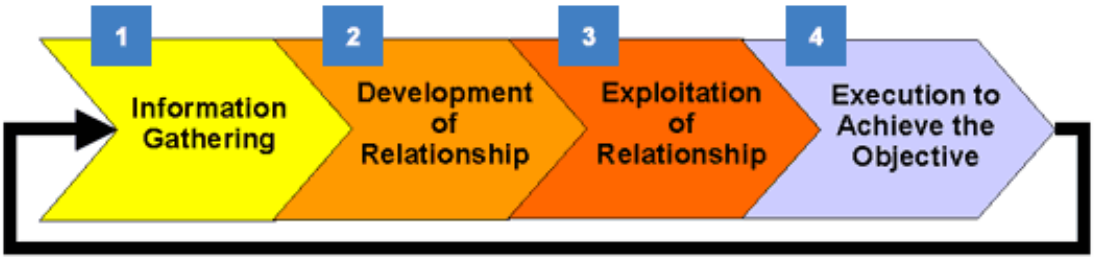
๑) รวบรวมข้อมูล (Information Gathering) เป็นขั้นตอนในการรวบรวมข้อมูลและรายละเอียดเกี่ยวกับเป้าหมายด้วยการสืบค้นหรือการสังเกต ซึ่งแหล่งของข้อมูลอาจมาจากเว็บไซต์ด้วยการใช้ Search Engine จากเครือข่ายสังคมออนไลน์ เช่น Facebook, Line (ขอเป็น

เพื่อนในกลุ่ม เพื่อคอยติดตามข้อมูลข่าวสาร) จากการประชุมสัมมนา, จากกิจกรรมประเภทอื่น หรือจากบุคคลใกล้ชิดและบุคคลที่มีความเกี่ยวข้องกับเป้าหมาย

๒) สร้างความสัมพันธ์ (Development of Relationship) เป็นขั้นตอนที่ผู้ปฏิบัติการเริ่มสร้างความสัมพันธ์ไปยังบุคคลเป้าหมาย ด้วยวิธีการขอสมัครเป็นเพื่อนในกลุ่มเครือข่ายสังคมออนไลน์ หรือสนทนาพูดคุยแบบ face-to-face โดยอาศัยโอกาสทางสังคมต่างๆ เช่น งานเลี้ยงขององค์กร หรือการประชุมสัมมนา เป็นต้น หรือการส่งอีเมลเพื่อแนะนำตัวและสร้างความสัมพันธ์ให้เกิดขึ้น (เช่น แจ้งว่าเคยพบกันในงานประชุมสัมมนาและเคยแลกเปลี่ยนนามบัตรกัน)

๓) ใช้ความสัมพันธ์ (Exploitation of Relationship) เป็นขั้นตอนที่ผู้ปฏิบัติการจะพยายามสร้างความสนิทสนมคุ้นเคยกับเป้าหมายให้มากยิ่งขึ้น พร้อมทั้งใช้ประโยชน์จากความสัมพันธ์นั้นในการให้ได้มาซึ่งข้อมูลที่ต้องการ หรือข้อมูลสำคัญอันจะเชื่อมโยงไปยังส่วนอื่นที่ต้องการได้ โดยอาศัยหลักการพื้นฐานทางมนุษยศาสตร์ดังกล่าวข้างต้น

๔) แสวงหาข้อมูลที่ต้องการ (Execution to Achieve the Objective) เป็นขั้นตอนในการนำข้อมูลที่ได้จากขั้นตอนที่ ๓ ไปใช้ในการโจมตีทางไซเบอร์ในรูปแบบต่างๆ เพื่อให้ได้มายังสิ่งที่ต้องการ



ภาพที่ ๑.๓๐ ขั้นตอนการปฏิบัติการ Social Engineering

๑.๓.๑๐.๓ ผลกระทบจาก Social Engineering ปฏิบัติการ Social Engineering สามารถส่งผลให้เกิดความเสียหายได้หลายรูปแบบและหลายระดับ ขึ้นอยู่กับวัตถุประสงค์และความหนักเบาของการปฏิบัติการ ดังนี้

๑) สูญเสียความเป็นส่วนบุคคล (Lack of Privacy) เป็นระดับที่มุ่งเป้าเฉพาะไปที่ตัวบุคคล ดังนั้นความเสียหายจะเกิดกับบุคคลในลักษณะที่ถูกคุกคามด้วยวิธีต่างๆ เช่น การได้รับเมล/ข้อความ/โพสต์ ประเภทโฆษณาหรือประกาศแจ้งเพื่อการพาณิชย์ต่างๆ รวมทั้งการถูกแอบอ้างนำชื่อเสียงไปใช้ในการสร้างประโยชน์ให้กับผู้ปฏิบัติการ Social Engineering (เช่น เชิญชวนให้กด Like/Share/Comment หรือนำภาพถ่ายไปใช้เพื่อแสวงหาประโยชน์)

๒) การเสื่อมเสียชื่อเสียง (Reputation) เป็นระดับที่มุ่งเป้าได้ทั้งตัวบุคคลและองค์กร โดยทำให้เกิดความเสื่อมเสียชื่อเสียงในสังคม และกระทบต่อการดำเนินชีวิตหรือการดำเนินภารกิจขององค์กร เช่น การแสวงหาข้อมูลและทำการโจมตีด้วยการเปลี่ยนหน้าเว็บไซต์

(Webpage Defacement) ของหน่วยงานภาครัฐ สามารถก่อให้เกิดความสูญเสียความไว้วางใจและความมั่นใจจากประชาชนในประเทศได้

๓) ความสูญเสียทางเศรษฐกิจและสังคม (Economic & Social Loss) เป็นระดับที่สร้างความเสียหายในรูปของตัวเงินด้านเศรษฐกิจหรือความมั่นคงทางสังคม โดยอาจมีมูลค่าได้มหาศาล เช่น การเจาะระบบฐานข้อมูลลูกค้าของบริษัทที่ทำธุรกิจด้านการเงินการธนาคาร และมีการโยกย้ายถ่ายโอนการเงินด้วยวิธีการเจาะระบบจากข้อมูลพื้นฐานสำคัญที่ได้มาจากการปฏิบัติการ Social Engineering การโจมตีเครื่องแม่ข่ายของผู้ให้บริการสำคัญต่างๆ แบบให้ปฏิเสธการให้บริการ (DDoS) เช่น การให้บริการด้านการเงิน การให้บริการภาครัฐ การให้บริการด้านสุขภาพ และการให้บริการด้านสื่อสารโทรคมนาคม เป็นต้น

๔) การปิดตัวขององค์กร (Closure) เป็นระดับที่มุ่งโจมตีสร้างความเสียหายหรือผลกระทบให้เกิดขึ้นในระดับที่องค์กรเป้าหมายต้องปิดตัวลง มักจะพบในแวดวงธุรกิจโดยเฉพาะองค์กรที่ถูกมองว่าเป็นคู่แข่งทางเศรษฐกิจ

๕) การเกิดคดีความทางกฎหมาย (Lawsuit) เป็นระดับที่มุ่งเป้าในการสร้างให้เกิดเป็นคดีความที่มีผลในเชิงกฎหมายขึ้นเพื่อประโยชน์ใด ๆ โดยจะปฏิบัติการเพื่อให้เกิดผลบังคับทางกฎหมายแก่เป้าหมาย เช่น การโจมตีบุคคลที่สามโดยปลอมแปลงและสร้างหลักฐานทางดิจิตัล (Digital Forensics) ว่าเป้าหมายเป็นผู้ปฏิบัติการ เป็นต้น ซึ่งในหลายกรณี ที่มีผลและก่อให้เกิดความเคลือบแคลงสงสัยในระดับโลก เช่น การพบว่าการโจมตีเจาะระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานในประเทศหนึ่ง มาจากปฏิบัติการของอีกประเทศหนึ่งอย่างต่อเนื่อง โดยความรุนแรงนี้อาจขยายผลไปสู่ระดับของการก่อการร้าย (Terrorism) ได้

แนวทางการป้องกันการทำวิศวกรรมสังคม (Social Engineering) สามารถปฏิบัติได้ดังนี้

๑) ไม่หลงเชื่อการหลอกลวง (Phishing) ทุกรูปแบบ
๒) ไม่เปิดเผยข้อมูลสำคัญส่วนบุคคลสู่สาธารณะ
๓) ไม่โพสต์ กิจกรรม สถานที่ทำงาน ตำแหน่งที่อยู่ ลงในสื่อสังคมออนไลน์
๔) ไม่พูดเรื่องงาน/เรื่องสำคัญที่เกี่ยวกับงานหรือระบบงานกับบุคคลทั่วไป

๑.๔ Peopleware กับการรักษาความปลอดภัย

เนื่องจากผลกระทบอันเกิดจากภัยคุกคามที่มากับเทคโนโลยีสารสนเทศนั้นสามารถสร้างความเสียหายให้เกิดขึ้นกับหน่วยงานคิดเป็นมูลค่าที่มีแนวโน้มที่จะเพิ่มขึ้นในทุกปี ทำให้หลายหน่วยงานต้องคิดแผนหรือมาตรการในการป้องกันและรักษาไว้ซึ่งความปลอดภัยของระบบสารสนเทศ ซึ่งโดยส่วนใหญ่มักเลือกที่จะลงทุนไปกับการสั่งซื้อและติดตั้งระบบป้องกันภัยคุกคามทางสารสนเทศในรูปแบบของ Hardware & Software ที่มีความทันสมัย มีประสิทธิภาพสูง และมีความแข็งแกร่งที่เพียงพอต่อการป้องกันภัยร้ายที่อาจแฝงตัวจากภายนอกเข้ามาในระบบในรูปแบบต่างๆ เช่น การติดตั้งระบบ Firewall เพื่อเป็นกำแพงป้องกันการถูกโจมตีจากภายนอก ทำให้การลงทุนประเภทนี้มักจะใช้งบประมาณที่มีมูลค่าสูง โดยหวังว่าจะมาช่วยลดความเสียหายอันอาจจะเกิดขึ้นกับองค์กรได้อย่างมีประสิทธิภาพ

ในอีกมุมหนึ่ง หลายหน่วยงานได้เลือกใช้วิธีกำหนดกฎเกณฑ์ กติกา ตลอดจนระเบียบปฏิบัติ ในการใช้งานคอมพิวเตอร์และข้อมูลในระบบสารสนเทศขององค์กร เพื่อเสริมมาตรการในการป้องกันความเสียหายอันอาจจะเกิดขึ้น โดยมักจะเป็นมาตรการเสริมควบคู่ไปกับการลงทุนป้องกันด้วย Hardware & Software โดยจะมีการระบุขั้นตอนการปฏิบัติไว้อย่างชัดเจน เช่น มาตรฐานในการตั้งค่ารหัสผ่าน การระมัดระวังไม่เปิดอีเมลที่ถูกส่งเข้ามาจากบุคคลภายนอกที่ไม่รู้จัก (โดยเฉพาะการไม่คลิกเปิดไฟล์แนบที่ไม่ทราบแหล่งที่มา) และ ขั้นตอนในการรับส่งข้อมูลที่มีชั้นความลับต่างๆ เป็นต้น

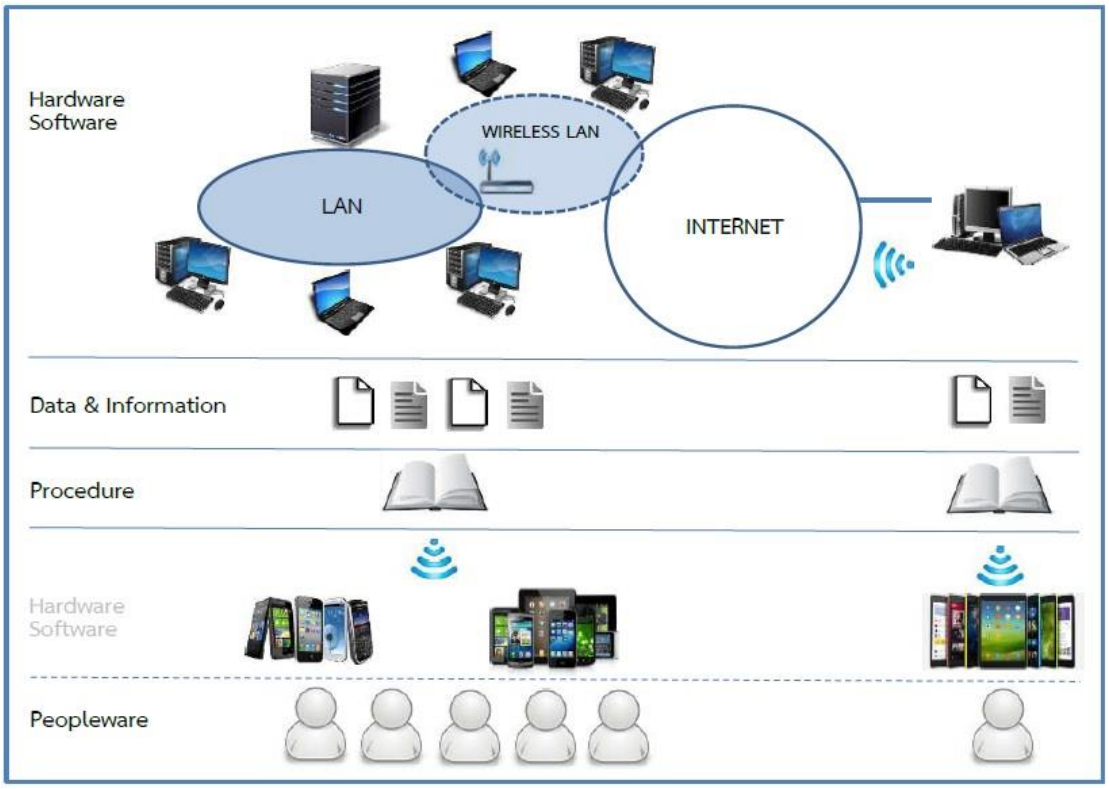
แต่ความเป็นจริงที่ปรากฏก็คือ พบว่ายังคงมีข่าวเกี่ยวกับความเสียหายที่เกิดขึ้นกับองค์กรหรือหน่วยงานชั้นนำทั้งภาครัฐและภาคเอกชน ปรากฏออกมาให้เห็นกันอยู่เสมอๆ และที่น่าแปลกใจไปกว่านั้นก็คือ หลายหน่วยงานด้านความมั่นคงชั้นนำในระดับประเทศ ต่างก็ล้วนแล้วแต่เคยได้รับความเสียหายจากการถูกโจมตีทางไซเบอร์ (Cyber Attack) มาแล้วทั้งสิ้น ทั้งๆที่มีการติดตั้งระบบในการป้องกันที่เรียกได้ว่าทันสมัยและทรงประสิทธิภาพ พร้อมระเบียบขั้นตอนการปฏิบัติที่มีความเข้มงวดและรัดกุมก็ตาม

ที่สร้างความตื่นตระหนกตกใจให้กับประเทศต่างๆ ทั่วโลก ก็คือ ข่าวการถูกโจมตีของระบบควบคุมการทำงานของโรงงานผลิตไฟฟ้าพลังนิวเคลียร์ที่ประเทศอิหร่าน โดยปฏิบัติการของเวิร์มที่ชื่อ Stuxnet ในปี 2010 ที่ผ่านมา ซึ่งการถูกโจมตีในครั้งนี้ได้รับการขนานนามว่าเป็นการอุบัติขึ้นครั้งแรกของ “สงครามไซเบอร์ (Cyber Warfare)” ในมวลมนุษยชาติ และที่น่าตกใจยิ่งไปกว่านั้นก็คือ การโจมตีเป้าหมายสำคัญทางยุทธศาสตร์ดังกล่าว ไม่ใช่การพยายามเจาะระบบจากภายนอกผ่านระบบป้องกันที่แน่นหนาของระบบควบคุมการทำงานที่มีความยากและซับซ้อนแต่อย่างใด หากแต่เป็นปฏิบัติการที่ใช้อาวุธและความพยายามเพียง **USB Flash Drive** เท่านั้น

“คน (Peopleware)” เป็นเหตุและปัจจัยสำคัญที่ก่อให้เกิดช่องโหว่ด้านความปลอดภัยต่างๆ เหล่านี้ โดยสามารถส่งผลกระทบในเชิงลบให้เกิดความเสียหายต่อหน่วยงานได้ แม้ว่าจะมีระบบในการป้องกันที่ทันสมัยอย่างเพียบพร้อมกับมาตรการที่เข้มงวดก็ตาม ซึ่งพบว่าเมื่อพิจารณาและวิเคราะห์ในเชิงวิชาการแล้ว “คน” หรือ “Peopleware” เป็น ๑ ในองค์ประกอบเชิงสารสนเทศของระบบสารสนเทศที่มีความเกี่ยวข้องกับอีก ๔ องค์ประกอบ ได้แก่ ฮาร์ดแวร์ (Hardware), ซอฟต์แวร์ (Software), กระบวนการหรือขั้นตอนการปฏิบัติ (Procedure) และ ข้อมูล/สารสนเทศ (Data, Information) อย่างมีนัยสำคัญ

ทั้งนี้ เมื่อวิเคราะห์องค์ประกอบทั้ง ๕ ของระบบสารสนเทศ ในบริบทของรูปแบบการใช้งานโดยทั่วไปของหน่วยงานส่วนใหญ่ในภาพรวมแล้ว จะสามารถเขียนผังอธิบายได้ ดังภาพที่ ๑.๓๑ ซึ่งจะเห็นว่า “บุคลากร (คน)” หรือ “Peopleware” จะมีส่วนเกี่ยวข้องกับอีก ๔ องค์ประกอบ (Hardware, Software, Data & Information, Procedure) อย่างมีนัยสำคัญที่จะส่งผลให้เกิดเป็นจุดอ่อนที่เปราะบางที่สุด (The Weakest Link) ได้ตลอดเวลา แม้ระบบคอมพิวเตอร์ของหน่วยงานจะมีระบบป้องกันที่แข็งแกร่ง ทันสมัย และมีระบบการเชื่อมต่อจากภายนอกแบบ VPN (Virtual Private Network) ที่ให้ความปลอดภัยสูงก็ตาม โดยมี Keyword ที่สำคัญ ๔ ตัว ตามรูปแบบการใช้งานทั่วไปที่มีความสะดวกและได้รับความนิยมสูงในปัจจุบัน ได้แก่ (๑) การเปิดบริการเชื่อมต่อแบบไร้สาย (Wi-Fi) ภายในองค์กร (๒) การอนุญาตให้นำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาใช้ในที่ทำงาน (BYOD: Bring Your Own Device) (๓) การเชื่อมต่อใช้งานระบบคอมพิวเตอร์ขององค์กรผ่านเครือข่ายอินเทอร์เน็ตไร้สายจากที่บ้าน และ (๔) การนำอุปกรณ์สื่อสารแบบพกพาประเภทสมาร์ท

โฟนและแท็บเล็ตมาเชื่อมต่อใช้งานข้อมูลภายในองค์กร (ทั้งเชื่อมต่อในที่ทำงานและเชื่อมต่อจากที่บ้าน) โดยสามารถวิเคราะห์จุดอันตรายอันเกิดจาก “คน” ภายใต้บริบทของการเป็น The Weakest Link ในเชิงวิชาการ ตามลำดับ Keyword ได้ ดังนี้



ภาพที่ ๑.๓๑ ความสัมพันธ์ของ Peopleware กับองค์ประกอบอื่น

(๑) การเปิดการเชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ขององค์กรแบบไร้สาย ให้ความสะดวกในด้านของการใช้งานเป็นอย่างยิ่ง เพราะสถานที่ในการใช้งานเครื่องคอมพิวเตอร์ (โดยเฉพาะแบบ Notebook) จะไม่ถูกจำกัดด้วยตำแหน่งของการเสียบสาย LAN แต่การเปิดใช้งานดังกล่าวจำเป็นต้องมีรหัสสำหรับการต่อเชื่อมใช้งานกับระบบ Wi-Fi นั้นๆ และอันตรายที่สำคัญซึ่งเกิดขึ้นได้อย่างง่ายดายก็คือ การรั่วไหลของรหัสเชื่อมต่อดังกล่าวอันเนื่องมาจากการจัดเก็บที่ไม่ปลอดภัยของผู้ใช้งาน (คน) เช่น เขียนรหัสเชื่อมต่อใส่กระดาษแปะติดไว้บนโต๊ะ หรือตัวคอมพิวเตอร์ Notebook ทำให้เมื่อใดก็ตามที่มีใครทราบรหัสและนำไปเชื่อมต่อกับระบบ Wi-Fi (สัญญาน Wi-Fi สามารถกระจายตัวได้ในบริเวณกว้าง ทำให้สามารถลักลอบเชื่อมต่อจากบริเวณใกล้เคียงได้) ก็จะสามารถเข้ามาเป็นหนึ่งในสมาชิกของเครือข่ายคอมพิวเตอร์ขององค์กรได้อย่างง่ายดาย โดยการเฝ้าคอยมอนิเตอร์เพื่อดูว่ามีใครแปลกปลอมเข้ามาใช้งานระบบเครือข่ายหรือไม่นั้น แทบจะเรียกได้ว่า ไม่มีการปฏิบัติเลยในองค์กรทั่วๆไปก็ว่าได้ นอกจากนี้ การเปลี่ยนรหัสเชื่อมต่อบ่อยๆ ตามวงรอบที่น่าจะมีการกำหนดตามแนวทางรักษาความปลอดภัยที่ระบุไว้ใน Procedure นั้น ก็เรียกได้ว่าแทบจะไม่มีการถือ

ปฏิบัติเลยในหน่วยงานทั่วไป เพราะคงทราบกันดีว่า เมื่อใดที่มีการเปลี่ยนรหัสเชื่อมต่อ เมื่อนั้นจะเกิดกระแสการ Complain จากเหล่าผู้ใช้งานเพราะเกิดความไม่สะดวกในทันที นอกจากนี้ อาจจะมีผู้ใช้งานในเครือข่ายบางคนที่ทำการแชร์ข้อมูลภายในวงไว้ด้วย (มักจะมีการแชร์ข้อมูลสำคัญระหว่างกันในเครือข่าย เพราะเป็นวัตถุประสงค์หลักของการตั้งระบบเครือข่ายภายในองค์กร) ซึ่งจุดนี้จะส่งผลให้ระบบสารสนเทศขององค์กรขาดคุณสมบัติของ Confidentiality (ซึ่งอาจรวมการสูญเสีย Integrity) ไปในทันทีอย่างง่ายดาย โดยไม่ต้องใช้ความพยายามในการเจาะข้อมูลที่มีความสลับซับซ้อนแต่อย่างใด

(๒) และ (๓) การอนุญาตให้ผู้ปฏิบัติงานสามารถนำอุปกรณ์คอมพิวเตอร์ส่วนตัวมาใช้ในสถานที่ทำงานได้ นับเป็นกระแสความสนใจในด้านการลด Cost ของหน่วยงาน กับความสะดวกในการทำงานกับอุปกรณ์คอมพิวเตอร์ของตัวเอง ที่มีข้อมูลเรื่องงานบรรจุอยู่และสามารถเรียกใช้ได้ตลอดเวลาอย่างสะดวก หากแต่ว่าจุดอันตรายที่เปราะบางก็คือ ผู้ใช้งานจะใช้เครื่องคอมพิวเตอร์เครื่องเดียวกันในการทำงานส่วนบุคคลซึ่ง (มักจะ) มีการเชื่อมต่อกับอินเทอร์เน็ตจากภายนอกอยู่ตลอดเวลา เช่น ที่บ้าน ซึ่งตรงนี้เอง Confidentiality จะขึ้นอยู่กับระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคลนั้นทันที (ซึ่งส่วนใหญ่มีเพียง By Default ทั่วไปเท่านั้น) ซึ่งจุดนี้ หมายรวมถึงการรักษารหัสเชื่อมต่อ Wi-Fi ของที่บ้านด้วย (หลายกรณี มักจะใช้เป็นหมายเลขโทรศัพท์มือถือ ซึ่งคาดเดาไม่ยาก) และ หากเครื่องคอมพิวเตอร์ดังกล่าวถูกใช้งานมากกว่าหนึ่งคนแล้วล่ะก็ คงมองเห็นภาพความสูญเสียคุณสมบัติข้อนี้ไปได้อย่างไม่ยากเลย ไม่ใช่แต่เพียงเท่านี้ ความเสี่ยงต่อการติดไวรัสหรือเวิร์ม ฯลฯ จากเครื่องคอมพิวเตอร์ส่วนบุคคล ขณะที่มีการนำเครื่องดังกล่าวมาเชื่อมต่อกับระบบเครือข่ายขององค์กร ก็มีสูงขึ้น เพราะระดับการป้องกันจะลดลงไปอยู่ที่ระดับของตัวบุคคลเท่านั้น และในกรณีที่เลวร้าย ไวรัสหรือเวิร์มดังกล่าวอาจส่งผลกระทบให้ระบบประมวลผลรวนข้อมูลเสียหายหรือสูญหาย หรือทำให้ระบบเครือข่ายไม่สามารถใช้งานได้ในวงกว้าง ทำให้สูญเสียคุณสมบัติของ Integrity & Availability อีกด้วย

(๔) อุปกรณ์สื่อสารแบบพกพาประเภทสมาร์ทโฟนและแท็บเล็ต ได้ขยายตัวอย่างรวดเร็ว ด้วยคุณสมบัติของ Performance และ Mobility ที่ให้ทั้งความสะดวกและตอบโจทย์การใช้งานแบบไม่จำกัดเวลาและสถานที่ ภายใต้ระดับราคาที่สามารถเอื้อมถึงได้ ทำให้อุปกรณ์พกพาดังกล่าวมีบทบาทเป็นอย่างมากในวิถีการดำเนินชีวิตในปัจจุบันของผู้คนทั่วไป และในหลายองค์กร ได้นำอุปกรณ์ดังกล่าวเข้ามาเป็นหนึ่งในเครื่องมือการปฏิบัติงานควบคู่ไปกับคอมพิวเตอร์ (หรือใช้แทนคอมพิวเตอร์ในหลายกรณี) ทำให้การเข้าถึงข้อมูลขององค์กรผ่านอุปกรณ์พกพาได้รับการถือปฏิบัติอย่างกว้างขวางมากขึ้นเป็นลำดับ ตรงจุดนี้ การรักษาความปลอดภัยของข้อมูลส่วนหนึ่งจะลดระดับลงมาที่ การรักษาความปลอดภัยของสมาร์ทโฟนและแท็บเล็ต ซึ่งหากเราสังเกตดีๆแล้ว ในหลายต่อหลายแอพพลิเคชั่นที่เราดาวน์โหลดใส่เข้าไปในอุปกรณ์พกพานั้น มีแจ้งเตือนเงื่อนไขที่ต้องอนุญาตให้แอพพลิชั่นนั้นๆ สามารถเข้าถึงข้อมูลต่างๆที่สำคัญได้ทั้งสิ้น เช่น ข้อมูล รูปภาพ, พิกัดตำแหน่ง, สมุดโทรศัพท์และบัญชีที่อยู่, ข้อมูลเอกสาร ฯลฯ ทำให้เราไม่สามารถที่จะควบคุมการรักษาคุณสมบัติ Confidentiality ของข้อมูลที่บรรจุได้เลย และจุดนี้เอง ที่มีการกล่าวขานว่าเป็นการขอข้อมูลสำคัญส่วนบุคคลแบบได้มาด้วยความละมุนละม่อม โดยไม่ต้องใช้ความพยายามใดๆในการเจาะข้อมูลเลย นอกจากนี้ ผู้ใช้หลายคนที่นิยมลงแอพพลิเคชั่นแปลกๆ ที่สุ่มเสี่ยงต่อการถูกโจรกรรมข้อมูลด้วยข้อเสนอที่ง่ายดาย

มาก เช่น ได้รับสติกเกอร์ฟรี ได้เกมส์ไว้เล่น เป็นต้น ความสุ่มเสี่ยงจะทวีคูณขึ้นไปอีกหากอุปกรณ์ต่างๆเหล่านั้น มีการแก้ไข ดัดแปลง เช่นมีการทำ Jail Break เป็นต้น

จะเห็นได้ชัดเจนว่า หากจะปิดจุดอ่อนอันเปราะบางที่เกิดจาก “คน” แล้ว มีความจำเป็นที่จะต้องใช้ความพยายามขั้นสูงในการที่จะสร้างความรู้และความเข้าใจที่เท่าทันต่อภัยในปัจจุบันที่อาจเข้ามาคุกคามและสร้างความเสียหายได้ทุกขณะ ภายใต้การสร้างความตระหนักถึงความปลอดภัยอย่างจริงจังให้กับบุคลากรทุกคนทุกระดับในหน่วยงาน ซึ่งในทางปฏิบัติแล้วเป็นสิ่งที่ปฏิบัติได้ยากถึงยากที่สุด โดยเฉพาะหน่วยงานที่มีผู้ปฏิบัติงานอยู่ในเจเนอเรชั่นเก่าที่ไม่มีความถนัดและรอบรู้อย่างเท่าทันในการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน (แต่มีสิทธิ์ในการใช้งานครบถ้วน) ดังนั้น ข้อมูลที่มีการรับส่งระหว่างกันภายใต้รูปแบบการใช้งานที่เต็มไปด้วยความเปราะบางอันเกิดจาก “คน” ไม่ควรเป็นข้อมูลที่อยู่ในชั้นความลับใดๆ หรือเป็นข้อมูลส่วนบุคคลที่มีความสำคัญ (เช่น เลขประจำตัวประชาชน, ข้อมูลการเงินและบัตรเครดิต ฯลฯ) แต่หากหน่วยงานใด มีความมั่นใจว่า “คน” ในระบบสารสนเทศ มีคุณภาพและรู้เท่าทันในเชิงปฏิบัติ ก็คงสามารถบริหารความเสี่ยงอันตรายต่างๆ เหล่านี้ได้อย่างมีประสิทธิผล

๑.๕ รหัสผ่าน (Password) และความปลอดภัย

“Password” หรือ “รหัสผ่าน” เป็นสิ่งที่จัดว่าอยู่ใกล้ตัวผู้ใช้บริการในโลกไซเบอร์มากที่สุดสิ่งหนึ่ง คงปฏิเสธไม่ได้ว่ามันคือกุญแจดอกสำคัญที่จะพาเราไปยังข้อมูลหรือบริการเฉพาะที่เป็นแบบส่วนบุคคลของเราได้อย่างปลอดภัย ไม่ว่าจะเป็น การใช้บริการบนอินเทอร์เน็ตแบบต่างๆ เช่น อีเมล เว็บไซต์ (ที่เป็นสมาชิก) ธุรกรรมการเงิน/ธนาคาร/บัตรเครดิตแบบออนไลน์ ระบบสื่อสารเครือข่ายสังคมออนไลน์ (MSN, Skype, Facebook ฯลฯ) หรือแม้กระทั่งการเปิดใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลของเรา ซึ่งทุกครั้งที่เราต้องการเข้าถึงความเป็นส่วนบุคคลดังกล่าว Password จะเป็นตัวที่ช่วยพิสูจน์ทราบความเป็นตัวตนที่แท้จริงของเราบนโลกไซเบอร์ได้ ไม่ว่าเราจะเชื่อมต่อเพื่อเข้าถึงข้อมูลหรือใช้บริการจากจุดใดก็ตามบนโลกใบนี้

การยืนยันถึงความเป็นตัวตนที่แท้จริงด้วย Password เป็นสิ่งที่สร้างความสะดวกสบายเป็นอย่างมาก เนื่องจากไม่สามารถที่จะแสดงบัตรประจำตัวประชาชนหรือบัตรแสดงตนอื่นๆ ได้ทุกที่และทุกครั้งที่เชื่อมต่อเพื่อเข้าใช้บริการ แต่ในขณะเดียวกัน เฉกเช่นเดียวกับดาบสองคม ความเป็นตัวตนอาจจะถูกปลอมแปลงหรือสวมสิทธิ์ได้โดยง่ายจากผู้ไม่ประสงค์ดี หากไม่ตั้งค่า Password ที่ให้ความปลอดภัยอย่างเพียงพอ มีผู้ใช้บริการระบบออนไลน์แบบต่างๆ เป็นจำนวนไม่น้อย ที่ได้รับความเสียหายอันเนื่องมาจาก Password ถูก Hack โดยไม่ทราบสาเหตุและไม่สามารถแกะรอยตามได้ คงจะเป็นสิ่งที่สามารถสร้างความเสียหายได้หากมันเกิดกับข้อมูลที่สำคัญ

ตรงนี้จะพิจารณาว่า Password นั้นมีลักษณะอย่างไร, ระดับความปลอดภัยหรือความไม่ปลอดภัยของ Password นั้นดูและวัดกันอย่างไร, Password ที่ใช้อยู่ในปัจจุบันมีความแข็งแกร่งที่ให้ความปลอดภัยเพียงพอหรือไม่ และ ทำอย่างไรจึงจะมั่นใจได้ว่า Password นั้นปลอดภัย

๑๕.๑ ลักษณะของ Password อาจอธิบายให้เข้าใจได้โดยง่ายว่า Password นั้นคือ “กลุ่มของตัวเลข ตัวอักษร หรือสัญลักษณ์ต่างๆ ที่เป็นความลับ ใช้สำหรับพิสูจน์ความเป็นตัวตนของบุคคล

ในการเข้าถึงข้อมูลหรือบริการ” ซึ่งจากความหมายนี้ ทำให้สามารถแบ่งแยกกลุ่มขององค์ประกอบใน Password ออกได้เป็น ๓ กลุ่มใหญ่ๆ (ภาพที่ ๑.๓๒) ได้แก่

Space	@	`
!	A	a
"	B	b
#	C	c
$	D	d
%	E	e
&	F	f
'	G	g
(	H	h
)	I	i
*	J	j
+	K	k
,	L	l
-	M	m
.	N	n
/	O	o
0	P	p
1	Q	q
2	R	r
3	S	s
4	T	t
5	U	u
6	V	v
7	W	w
8	X	x
9	Y	y
:	Z	z
;	[	{
<	\	|
=	]	}
>	^	~
?	_	

ภาพที่ ๑.๓๒ องค์ประกอบของ Password

๑๕.๑.๑ กลุ่มตัวเลข ประกอบไปด้วยตัวเลข 0~9 จำนวน ๑๐ ตัว (ส่วนที่ระบายด้วยสีเหลือง)

๑๕.๑.๒ กลุ่มตัวอักษร ประกอบไปด้วย a, b, c, ..., x, y, z และ A, B, C, ..., X, Y, Z (กรณีแยกความแตกต่างระหว่างอักษรตัวเล็กและตัวพิมพ์ใหญ่) จำนวน ๕๒ ตัว (ส่วนที่ระบายด้วยสีฟ้า)

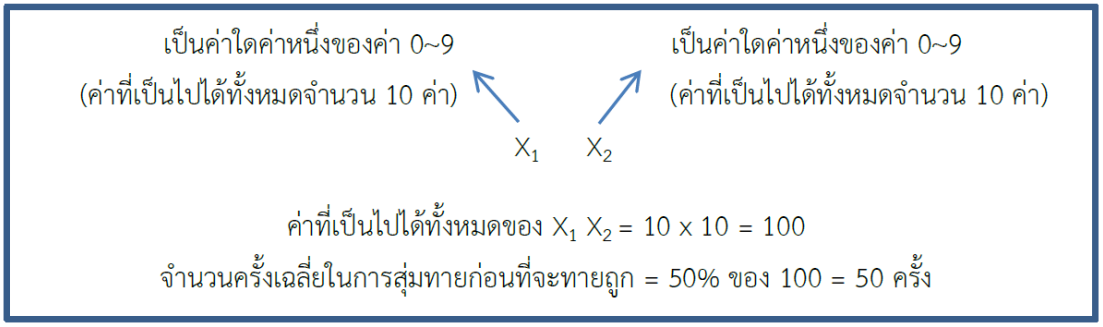
๑๕.๑.๓ กลุ่มสัญลักษณ์ ประกอบไปด้วยสัญลักษณ์ต่างๆ ที่สามารถพิมพ์ผ่านแป้นคีย์บอร์ดได้ เช่น *, -, +, # เป็นต้น จำนวน ๓๓ ตัว (รวม Space) (ส่วนที่ระบายด้วยสีแดง)

โดยปกติ Password ควรจะประกอบไปด้วยการผสมผสานของ ตัวเลข ตัวอักษร และสัญลักษณ์ ที่เลือกมาจากในแต่ละกลุ่ม เช่น “Pol_191#”, “bom27+mod25” และ “logo&me7-11” เป็นต้น แต่มีผู้ใช้งานจำนวนไม่น้อยเลือกที่จะตั้ง Password ของตัวเองจากกลุ่มของตัวเลขเพียงอย่างเดียว เช่น ตั้งเป็นหมายเลขโทรศัพท์มือถือของตัวเอง และมีผู้ใช้งานจำนวนไม่น้อยอีกเช่นกัน ที่เลือกที่จะตั้ง Password ของตัวเองเป็นคำที่เลือกจากสมาชิกของกลุ่มตัวอักษรเพียวอย่างเดียว เช่น “nihongo”, “iamsam” และ “lamos” เป็นต้น โดยในหลายกรณีที่ผู้ใช้งานเลือกที่จะตั้ง Password ของตัวเองเป็นคำศัพท์ต่างๆ ที่สั้นและง่ายต่อการจดจำ เช่น “bird”, “cat”, “book” และ “beautiful”

ในทางปฏิบัติจริงแล้ว หลายคนประสงค์ที่จะตั้ง Password ของตัวเองให้เป็นสิ่งที่ตัวเองสามารถที่จะจดจำได้ง่ายหรือเป็นสิ่งที่มีความหมายพิเศษกับตัวเอง เช่น ชื่อของคนรัก ชื่อของเพื่อนสนิท วันเดือนปีเกิดของตัวเอง เลขบัตรประจำตัวต่างๆ หรือแม้แต่คำศัพท์ทั่วไปในภาษาอังกฤษ โดยหลีกเลี่ยงที่จะตั้ง Password ด้วยการผสมผสานของสมาชิกจากกลุ่มต่างๆ ทั้ง ๓ กลุ่มดังกล่าวข้างต้น ด้วยเหตุผลว่า “ยากต่อการจดจำ” แต่ปัญหาหนึ่งที่เกิดขึ้นและเกิดขึ้นจริงอยู่บ่อยๆ ก็คือการถูก Hack ค่า Password ไปโดยง่ายและเกิดความสูญเสียหรือเสียหายขึ้นจากการถูกลักลอบใช้งานด้วยการสวมสิทธิ์ดังกล่าวจากผู้ไม่ประสงค์ดี โดยปัญหาดังกล่าวจะทวีความรุนแรงขึ้น หากเกิดกับด้านธุรกรรมการเงิน การธนาคาร การบัญชี ความลับส่วนบุคคล และความมั่นคงปลอดภัยของชีวิตและทรัพย์สิน

๑๕.๒ ระดับความปลอดภัยของ Password สมมุติให้นึกตัวเลข ๑ ตัวไว้ในใจ แล้วให้เพื่อนทายตัวเลขนั้นจนกว่าจะถูก จำนวนครั้งที่เพื่อนจะทายสูงสุดจนกว่าจะทายถูกในกรณีเลวร้ายที่สุด (Worst Case) ก็คือ ๑๐ ครั้ง ซึ่งหมายถึงลองสุ่มทายทุกค่าของตัวเลขที่มีความเป็นไปได้ (Brute Force Attack) นั่นก็คือตั้งแต่เลข 0 ถึงเลข 9 โดยตัวเลขที่ทายตัวสุดท้ายเป็นตัวที่ถูกต้อง โดยจะมีค่าเฉลี่ยจำนวนครั้งในการทายก่อนที่จะทายถูกอยู่ที่ ๕ ครั้ง หรือ ๕๐ % ของจำนวนตัวเลขที่เป็นไปได้ทั้งหมด ในกรณีเดียวกัน หากเป็นตัวเลข ๒ หลัก เพื่อนก็จะต้องทาย (Worst Case) เป็นจำนวนสูงสุดถึง ๑๐๐ ครั้ง (00~99) โดยจะมีค่าเฉลี่ยจำนวนครั้งในการทายก่อนที่จะทายถูกอยู่ที่ ๕๐ ครั้ง ซึ่งจำนวนครั้งเฉลี่ยในการสุ่มทายก่อนที่จะทายถูกนี้เอง ที่เป็นตัววัดค่าความปลอดภัยของตัวเลขที่นึกอยู่ในใจ โดยค่าตัวเลขที่มีหลายหลักมากเท่าใด ความปลอดภัยในการที่จะไม่ถูกเพื่อนทายถูกก็จะยิ่งเพิ่มเป็นสัดส่วนทวีคูณมากขึ้นเท่านั้น

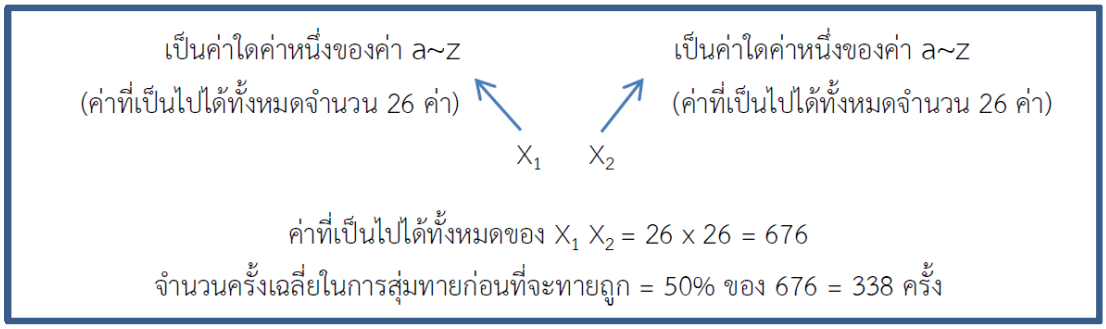
สัดส่วนทวีคูณ ที่ว่านั้นสามารถเขียนอธิบายให้เข้าใจง่ายๆ ได้ดังนี้ สมมุติให้ X_1, X_2 เป็นค่าตัวเลขแต่ละหลักของตัวเลข ๒ หลัก (ภาพที่ ๑.๓๓)



ภาพที่ ๑.๓๓ สัดส่วนทวีคูณของ Password (ค่า 0 - 9)

ในลักษณะเดียวกัน หากเป็นตัวเลข ๘ หลัก ก็จะได้ค่าที่เป็นไปได้ทั้งหมดของ $X_1\ X_2\ X_3\ X_4\ X_5\ X_6\ X_7\ X_8 = 10^8 = 100,000,000$ โดยมีจำนวนครั้งเฉลี่ยในการสุ่มทายก่อนที่จะทายถูกเท่ากับ 50,000,000 ครั้ง

หากเปลี่ยนค่า $X_1\ X_2$ เป็นค่าของตัวอักษรภาษาอังกฤษตัวเล็ก (a~z) จะได้ ดังนี้ (ภาพที่ ๑.๓๔)



ภาพที่ ๑.๓๔ สัดส่วนทวีคูณของ Password (ค่า a - z)

ในลักษณะเดียวกัน หากเป็นตัวอักษรภาษาอังกฤษเล็กจำนวน ๘ หลัก ก็จะได้ค่าที่เป็นไปได้ทั้งหมดของ $X_1\ X_2\ X_3\ X_4\ X_5\ X_6\ X_7\ X_8 = 26^8 = 208,827,064,576$ โดยมีจำนวนครั้งเฉลี่ยในการสุ่มทายก่อนที่จะทายถูกเท่ากับ 104,413,532,288 ครั้ง และหากเป็นตัวอักษรภาษาอังกฤษเล็กและตัวพิมพ์ใหญ่จำนวน ๘ หลัก ก็จะได้ค่าที่เป็นไปได้ทั้งหมดของ $X_1\ X_2\ X_3\ X_4\ X_5\ X_6\ X_7\ X_8 = 52^8 = 53,459,728,531,456$ โดยมีจำนวนครั้งเฉลี่ยในการสุ่มทายก่อนที่จะทายถูกเท่ากับ 26,729,864,265,728 ครั้ง

จะเห็นได้ว่าระดับความปลอดภัยของการที่จะไม่ถูกทายค่าที่คิดไว้ถูก จะขึ้นอยู่กับปัจจัยหลักๆ ๒ ปัจจัย ได้แก่ **“ความยาว** (หรือปริมาณ)” ของค่าที่คิดไว้ กับ “**ค่าที่เป็นไปได้ทั้งหมดของแต่ละหลัก**” (X_i) นั่นคือ ยิ่งมีหลายหลัก (หลายตำแหน่ง) มากเท่าใด และแต่ละหลัก (แต่ละตำแหน่ง) มีค่าความเป็นไปได้มากเท่าใด ระดับของความปลอดภัยก็จะมากขึ้นไปด้วย

หากใช้คอมพิวเตอร์ที่มีความเร็วในการประมวลผล 2.4 GHz มาใช้ในการสุ่มทายค่าที่คิดไว้ดังกล่าว โดยอนุมานให้สัญญาณนาฬิกาแต่ละรอบ (Hz) สามารถทำงาน ๑ รอบคำสั่งที่คำนวณความถูกต้องของค่าที่ทายสุ่มได้ คอมพิวเตอร์ก็จะสามารถทายค่าได้ถึง 2,400,000,000 ค่า ในเวลา ๑ วินาที นั่นคือสามารถคำนวณหาค่าที่ถูกต้อง (โดยเฉลี่ยในการสุ่มทาย) ของ Password ที่เป็นตัวอักษรภาษาอังกฤษเล็ก ๘ หลัก ได้ในเวลา ๔๓.๕ วินาที และสามารถคำนวณหาค่าที่ถูกต้อง (โดยเฉลี่ยในการสุ่มทาย) ของ Password ที่เป็นตัวอักษรภาษาอังกฤษเล็กและตัวพิมพ์ใหญ่ ๘ หลัก ได้ในเวลา ๓ ชั่วโมงเศษ

หากตั้งค่า Password แต่ละตำแหน่งด้วยค่าที่เป็นไปได้ทั้ง ตัวเลข ตัวอักษร (ตัวเล็กและตัวพิมพ์ใหญ่) และสัญลักษณ์ต่างๆ (ตามภาพที่ ๑.๓๒) ก็จะได้ค่าที่เป็นไปได้ทั้งหมดของแต่ละตำแหน่งเพิ่มขึ้นเป็น 95 (มาจาก 10+52+33) ซึ่งทำให้ค่าที่เป็นไปได้ทั้งหมดของ Password ที่มีความยาว L ($X_1\ X_2\ X_3\ \ldots\ X_{L-2}\ X_{L-1}\ X_L$) ตำแหน่ง เท่ากับ 95^L และจำนวนครั้งเฉลี่ยในการสุ่มทายก่อนที่จะทายถูกเท่ากับ ครึ่งหนึ่งของ 95^L ครั้ง ซึ่งหาก Password มีความยาว ๘ ตำแหน่ง จะได้ค่าที่เป็นไปได้ทั้งหมดของ $X_1\ X_2\ X_3\ X_4\ X_5\ X_6\ X_7\ X_8 = 95^8 = 6,634,204,312,890,625$ โดยมีจำนวนครั้งเฉลี่ยในการสุ่มทายก่อนที่จะทายถูกเท่ากับ 3,317,102,156,445,312.5 ครั้ง ทำให้การสุ่มทายจากคอมพิวเตอร์ที่มีความเร็วในการประมวลผล 2.4 GHz ต้องใช้เวลาถึงกว่า ๓๘๓ ชั่วโมง (เกือบ ๑๖ วัน) โดยเฉลี่ย จึงจะสุ่มทายค่าได้ถูก และหากตั้งค่าของ Password ให้มีความยาวถึง ๑๖ หลัก (เช่น ความยาวสูงสุดของ Password ที่ตั้งได้ใน Hotmail) ก็จะต้องใช้เวลาเฉลี่ยในการสุ่มทายค่าให้ถูกต้องถึงกว่า ๒๙๔ ล้านล้านปีทีเดียว

อย่างไรก็ตาม ในบางระบบความปลอดภัย อาจมีข้อจำกัดเรื่องการตั้งค่า Password เพิ่มเข้ามา เช่น ห้ามตั้งค่า ๓ หลักแรกของ Password เหมือนกับค่า ๓ หลักแรกของชื่อผู้ใช้ (User Name) หรือ ไม่ให้นำบางค่าในกลุ่มของสัญลักษณ์ไปใช้เป็นองค์ประกอบของ Password เช่น Space, ‘ (Single Quote), และ “ (Double Quote) เป็นต้น ทำให้การคำนวณเวลาเฉลี่ยอาจมีการเปลี่ยนแปลงไปบ้างตามเงื่อนไขที่เพิ่มขึ้นนั้นๆ

จริงๆ แล้ว ในเชิงวิชาการ ค่าความปลอดภัยของ Password จะถูกวัดออกมาเป็นค่าของ Entropy ในหน่วยของ bits ตามหลักของทฤษฎีสารสนเทศ (Information Entropy) ซึ่งแสดงถึงความไม่แน่นอนที่ผูกกับตัวแปรสุ่ม กล่าวคือยิ่งค่า Entropy มีค่าสูงขึ้น ค่าความไม่แน่นอนของตัวแปรสุ่มก็จะสูงขึ้นตาม ทำให้การคาดคะเนค่าที่จะออกมากระทำได้ยากขึ้น โดยค่า Entropy ของ Password ที่มีความยาว L (เช่น $X_1\ X_2\ X_3\ \ldots\ X_{L-2}\ X_{L-1}\ X_L$) ซึ่งค่าในแต่ละหลัก (ค่า X_i ใดๆ) ของ Password ถูกสุ่มเลือกมาจากกลุ่มของค่าที่มีจำนวนค่าที่เป็นไปได้ทั้งหมด N ค่า มีค่าเท่ากับ “$L \log_2 N$” ทำให้ค่า Entropy ต่อ 1 หลักความยาวของ Password แยกตามชนิดของกลุ่มองค์ประกอบเป็นดังนี้ (ตารางที่ ๑.๒)

ตารางที่ ๑.๒ ค่า Entropy ของ Password

ประเภทกลุ่ม	จำนวนค่าที่เป็นไปได้ทั้งหมดในกลุ่ม	ค่า Entropy ต่อความยาว 1 ตำแหน่ง
ตัวเลข 0~9	10	3.3219 bits
ตัวอักษร a~z และ A~Z	52	5.7004 bits
สัญลักษณ์ต่างๆ	33	5.0448 bits
ตัวเลข 0~9 กับ ตัวอักษร a~z และ A~Z	62	5.9542 bits
ตัวเลข 0~9 กับ ตัวอักษร a~z และ A~Z กับ สัญลักษณ์ต่างๆ	95	6.5699 bits

จากค่า Entropy ของแต่ละตำแหน่งที่ระบุในตารางที่ ๑.๒ ทำให้สามารถคำนวณค่า Entropy ของ Password ที่มีความยาว ๘ หลัก ที่สร้างจากกลุ่มค่าต่างๆ (จากในภาพที่ ๑.๓๒) ได้ดังนี้ (ตารางที่ ๑.๓)

ตารางที่ ๑.๓ ค่า Entropy ของ Password ๘ ตำแหน่ง

ประเภทกลุ่ม	ค่า Entropy ของ Password ๘ ตำแหน่ง
ตัวเลข 0~9	26.5752 bits
ตัวอักษร a~z และ A~Z	45.6032 bits
สัญลักษณ์ต่างๆ	40.3584 bits
ตัวเลข 0~9 กับ ตัวอักษร a~z และ A~Z	47.6336 bits
ตัวเลข 0~9 กับ ตัวอักษร a~z และ A~Z กับ สัญลักษณ์ต่างๆ	52.5592 bits

สำหรับช่วงของตัวเลขค่า Entropy ที่บ่งบอกถึงระดับความปลอดภัยของ Password นั้น โดยสากลทั่วไปสามารถจำแนกได้ ดังนี้ (ตารางที่ ๑.๔)

ตารางที่ ๑.๔ ค่า Entropy กับระดับความปลอดภัยของ Password

ค่า Entropy	ระดับความปลอดภัย
น้อยกว่า 28 bits	ต่ำมาก (ระดับใช้ป้องกันคนในครอบครัว เช่น Security Code ของ Smart Phone)
28~35 bits	ต่ำ (ระดับใช้ป้องกันคนในที่ทำงาน เช่น Password สำหรับ Login เข้าคอมพิวเตอร์)
36~59 bits	พอใช้ (ระดับใช้เป็น Password สำหรับ Login เข้าสู่ระบบเครือข่ายในที่ทำงาน)
60~127 bits	แข็งแกร่ง (ระดับใช้ป้องกันข้อมูลด้านการเงินและบัญชี)
ตั้งแต่ 128 bits ขึ้นไป	แข็งแกร่งมาก (ระดับป้องกันการ Hack ได้อย่างมีประสิทธิภาพสูง)

นั่นคือ ค่า Entropy ของ Password ที่ตั้งขึ้นไม่ควรต่ำกว่า 36 bits โดยรวม และหากเป็นไปได้ ควรมีค่าสูงถึงตั้งแต่ 60 bits ขึ้นไป เพื่อความปลอดภัยที่สูงขึ้น ทั้งนี้เมื่อพิจารณา Password ที่มีความยาวจำนวน ๘ ตำแหน่ง ที่สร้างขึ้นจากกลุ่มข้อมูลดังแสดงในตารางที่ ๑.๓ แล้ว จะพบว่า Password ความยาว ๘ ตำแหน่งที่เข้าข่ายมีความแข็งแกร่งพอใช้นั้นก็คือ Password ที่สร้างขึ้นจากกลุ่มผสมของตัวเลข 0~9 กับ ตัวอักษร a~z และ A~Z กับ สัญลักษณ์ต่างๆ รวมกัน อย่างไรก็ตาม การตั้งค่าให้ Password มีความยาวที่มากขึ้นกว่า ๘ ตำแหน่งจะทำให้ Password นั้นมีความแข็งแกร่งที่มากขึ้นได้อีก สำหรับระดับของความปลอดภัยแนะนำ ที่หน่วยงาน NIST (National Institute of Standard and Technology) ของสหรัฐอเมริการะบุไว้ก็คือ ระดับ 80 bits หรือ Password ที่ตั้งแบบสุ่มจาก ตัวเลข ตัวอักษร และสัญลักษณ์ ทั้ง ๓ กลุ่ม ที่มีความยาวตั้งแต่ ๑๒ ตำแหน่งขึ้นไป

ทั้งนี้และทั้งนั้น ความนานของการคำนวณเวลาเฉลี่ยในการสุ่มทายค่าให้ถูกต้อง และค่าของ Entropy ดังกล่าวนั้น อยู่บนพื้นฐานของทฤษฎีภายใต้การตั้ง Password จากการ **“สุ่มเลือกค่า (Randomization)”** ที่เป็นไปได้ทั้งหมดจากแต่ละกลุ่ม (ตัวเลข ตัวอักษร และสัญลักษณ์) ซึ่งหมายถึงว่า หาก Password ใดถูกตั้งขึ้นแบบจงใจภายใต้กฎเกณฑ์เฉพาะของแต่ละบุคคล (เช่น ต้องจำง่ายและมีความหมายพิเศษต่อตัวเอง หรือเป็นคำศัพท์มีความหมายที่มีการใช้งานอยู่โดยทั่วไป) แล้วละก็ การคาดคะเนค่าของ Password ก็สามารถที่กระทำได้ง่ายขึ้น และในปัจจุบัน มีเทคนิคจำนวนมากที่ถูกนำเสนอเพื่อประกอบการคาดคะเน (ทายค่าที่ถูกต้อง) Password ดังกล่าว เช่น การใช้เทคนิคการถอด Password ด้วยวิธีทดสอบคำศัพท์ในพจนานุกรม (Dictionary Attack) และการวิเคราะห์จากสถิติการตั้งค่า Password โดยทั่วไป (Human-Generated Passwords Analysis) เป็นต้น โดยในกรณีที่ตั้ง Password เป็นคำศัพท์ที่มีปรากฏอยู่ในพจนานุกรม การ Hack ค่า Password ก็สามารถกระทำได้โดยง่ายและรวดเร็วด้วยการทดสอบคำศัพท์ทั้งหมด (ซึ่งมีปริมาณน้อยและจำกัด) ที่มีอยู่ทั้งหมดในพจนานุกรม โดยเวลาที่ใช้ในการ Hack ค่าของ Password นี้ สั้นเพียงระดับเสี้ยววินาทีเท่านั้น

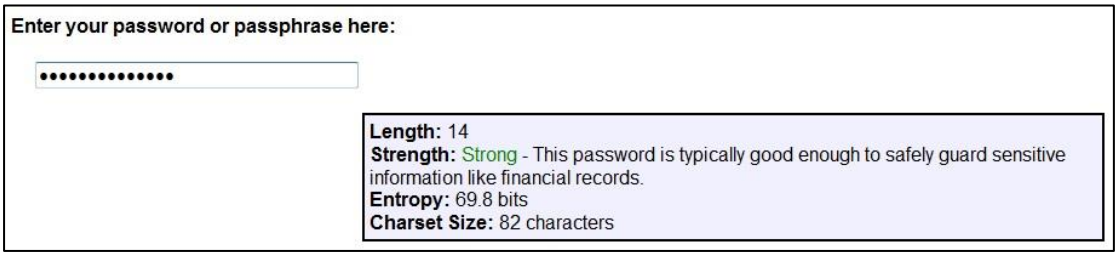
ในทางปฏิบัติจริง ผู้ใช้งานมักจะไม่มีผู้ใดที่ตั้งค่า Password ของตัวเองแบบสุ่ม เพราะจะทำให้ยากต่อการจดจำมาก เนื่องจากค่า Password ที่ได้จากการสุ่มนั้นมักจะไม่สื่อถึงความหมายใดๆ ที่เอื้อต่อการจดจำเลย ตรงกันข้าม ผู้ใช้งานพยายามที่จะเลือกตั้งค่า Password ของตัวเองแบบที่สื่อและมีความหมายพิเศษกับตัวเองมากกว่า และสิ่งที่สามารถให้ความร่วมมือในการยกระดับความปลอดภัยของ Password ได้ก็คือ การพยายามที่จะเลือกตั้งค่าของ Password ให้ประกอบไปด้วยค่าทั้ง ๓ ค่าของตัวเลข ตัวอักษร และค่าของสัญลักษณ์ ที่รวมกันแล้วสื่อความหมายพิเศษที่จดจำง่ายแก่ตัวเองให้มากที่สุดเท่าที่จะทำได้เท่านั้น แต่ทั้งนี้ หากการตั้งค่า Password ไม่เกิดจากการสุ่มที่แท้จริงแล้ว สิ่งหนึ่งที่จะสามารถชดเชยให้ระดับความปลอดภัยของ Password สูงขึ้นได้ก็คือ การตั้ง Password ให้มีความยาวที่มากขึ้นนั่นเอง

๑.๕.๓ ตรวจสอบระดับความปลอดภัยของ Password ในการตรวจสอบว่า Password ปัจจุบันที่ใช้งานอยู่นั้น มีค่าระดับของความปลอดภัยมากน้อยเพียงใด เพื่อประกอบการตัดสินใจในการเปลี่ยนไปตั้งค่า Password ใหม่ ซึ่งการทดสอบระดับความปลอดภัยของ Password ดังกล่าวนั้นสามารถกระทำแบบออนไลน์ผ่านเว็บไซต์ที่เปิดให้บริการในการตรวจสอบได้ทันทีตลอดเวลา เช่น

http://www.passwordmeter.com/
http://howsecuremypassword.net/
http://rumkin.com/tools/password/passchk.php

ตัวอย่างของผลการตรวจสอบระดับความปลอดภัยของ Password ผ่านช่องทางทั้ง ๓ เว็บไซต์ที่เปิดให้บริการดังกล่าว โดยใช้ Password ตัวอย่างที่มีความยาว ๑๔ ตำแหน่ง ประกอบไปด้วยสมาชิกที่เลือกมาจากทั้ง ๓ กลุ่ม ได้แก่ กลุ่มตัวเลข กลุ่มตัวอักษร และกลุ่มสัญลักษณ์ (ใช้ Password ตัวเดียวกันกับทั้ง ๓ เว็บไซต์) แสดงได้ดังภาพที่ ๑.๓๕

http://www.passwordmeter.com/



http://howsecuremypassword.net/

http://rumkin.com/tools/password/passchk.php

ภาพที่ ๑.๓๕ ผลการตรวจสอบระดับความปลอดภัยของ Password ตัวอย่าง (๑๔ หลัก)

๑.๕.๔ การตั้งค่า Password ที่เหมาะสม เพื่อสร้างความมั่นใจใน Password ที่จะใช้ปกป้องการเข้าถึงข้อมูลหรือบริการเฉพาะที่เป็นแบบส่วนบุคคลได้อย่างปลอดภัย แนะนำให้ใส่ใจกับสิ่งต่อไปนี้เป็นพิเศษทุกครั้งที่มีการตั้งค่า Password ใช้งาน

๑.๕.๔.๑ ความยาวควรไม่ต่ำกว่า ๘-๑๐ ตำแหน่งหากเป็นไปได้

๑.๕.๔.๒ ไม่ควรมีส่วนของคำศัพท์ในพจนานุกรมเป็นองค์ประกอบ

๑.๕.๔.๓ ประกอบไปด้วยสมาชิกครบจากทั้ง ๓ กลุ่ม (ตัวเลข, ตัวอักษร, สัญลักษณ์)

๑.๕.๔.๔ ในส่วนของตัวอักษร ควรประกอบไปด้วยทั้งอักษรตัวเล็กและตัวพิมพ์ใหญ่

๑.๕.๔.๕ ไม่มีชุดของสมาชิกตัวเลขที่เป็นเอกลักษณ์เด่น เช่น “007”, “191” และ “7-11” เป็นต้น

๑.๕.๔.๖ ไม่เรียงลำดับในลักษณะของ Pattern ยอดนิยม เช่น ตัวอักษรตามด้วยตัวเลข (boon1981, kai12062528 ฯลฯ) หรืออักษรตัวแรกจะต้องเป็นตัวพิมพ์ใหญ่ (SoomsakFire, LoveYou ฯลฯ)

๑.๕.๔.๗ ไม่ประกอบด้วยข้อมูลส่วนบุคคลทั่วไป เช่น วันเดือนปีเกิด สถานที่ทำงาน หมายเลขบัตร ชื่อตัวหรือชื่อสกุล เป็นต้น

๑.๕.๔.๘ หลีกเลี่ยงการใช้ตัวอักษรซ้ำๆ เช่น yymm9911

นอกจากนี้ การตระหนักอยู่เสมอว่าควรเก็บรักษา Password ของตนเองไว้เป็นความลับ ถือเป็นสิ่งที่ **สำคัญที่สุด**

๑.๖ การบูรณาการอุปกรณ์ BYOD กับการรักษาความปลอดภัย

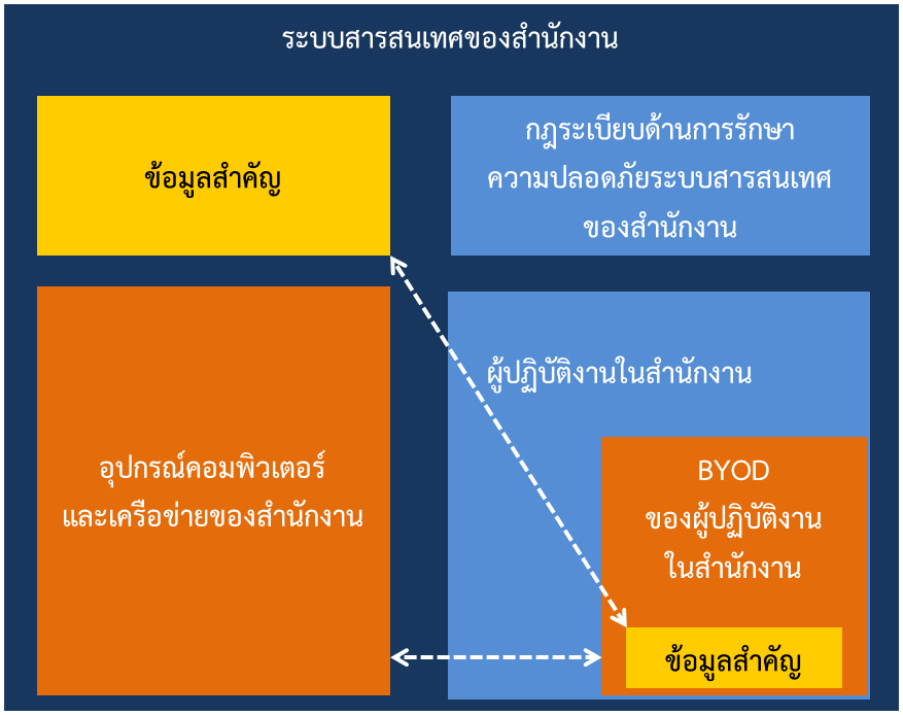
ปัจจุบัน มีผู้ปฏิบัติงานในหน่วยงานจำนวนมากที่นำอุปกรณ์ส่วนบุคคลประเภท คอมพิวเตอร์โน้ตบุ๊ค สมาร์ทโฟน แท็บเล็ท ตลอดจนอุปกรณ์บันทึกข้อมูลแบบพกพา (USB Flash Drive, External Harddisk) และอุปกรณ์ Internet of Things (IoT) มาใช้ปฏิบัติงานในหน่วยงานร่วมกับอุปกรณ์คอมพิวเตอร์และเครือข่ายของหน่วยงาน ในลักษณะของ Bring Your Own Device (**BYOD**) เนื่องจากความสะดวกในการพกพาและสามารถปฏิบัติงานที่บ้านได้อย่างต่อเนื่องหลังเวลาทำงานปกติอีกด้วย นอกจากนี้ ในแง่ของหน่วยงานแล้ว เป็นช่องทางในการลดภาระค่าใช้จ่ายในการจัดสรรทรัพยากรด้านสารสนเทศเพิ่มเติมอีกด้วย

อย่างไรก็ตาม ในการอนุญาตให้ผู้ปฏิบัติงานนำอุปกรณ์ส่วนบุคคลในลักษณะของ BYOD มาใช้ร่วมกับทรัพยากรด้านสารสนเทศอื่นของหน่วยงานนั้น หมายถึง อุปกรณ์ BYOD จะเข้ามารวมอยู่ในกลุ่มองค์ประกอบระบบสารสนเทศหน่วยงานด้วย จึงมีความจำเป็นอย่างยิ่งที่จะต้องคำนึงถึงคุณสมบัติด้านความปลอดภัยของระบบสารสนเทศหน่วยงานเพิ่มเติม (ภาพที่ ๑.๓๖)

แนวคิดการรักษาความปลอดภัยระบบสารสนเทศหน่วยงาน กรณีบูรณาการอุปกรณ์ BYOD เข้ากับระบบสารสนเทศของหน่วยงานแบ่งเป็น ๒ ด้าน (ภาพที่ ๑.๓๗) ดังนี้

<table>
<tr><td colspan="5">ระบบสารสนเทศ</td></tr>
<tr><td>Hardware</td><td>Software</td><td>Data</td><td>People</td><td>Procedures</td></tr>
<tr><td colspan="3">Computer Network + BYOD, Telecommunication, Software, Database</td><td>People</td><td>Procedures</td></tr>
<tr><td colspan="3">Data Confidentiality, Data Integrity, System Availability</td><td>Privacy, Non-Repudiation</td><td></td></tr>
<tr><td colspan="3">เทคโนโลยี</td><td>บุคลากร</td><td>กระบวนการ</td></tr>
</table>

ภาพที่ ๑.๓๖ อุปกรณ์ BYOD ที่รวมอยู่ในกลุ่มองค์ประกอบของระบบสารสนเทศหน่วยงาน



ภาพที่ ๑.๓๗ กรอบแนวคิดการบูรณาการอุปกรณ์ BYOD กับการรักษาความปลอดภัย

๑.๖.๑ การเชื่อมต่ออุปกรณ์ BYOD เข้ากับระบบเครือข่ายสารสนเทศของหน่วยงาน

อุปกรณ์ BYOD จะมีการเชื่อมต่อเข้ากับระบบคอมพิวเตอร์และเครือข่ายสารสนเทศของหน่วยงานเพื่อการเรียกใช้ทรัพยากรสารสนเทศจากระบบสารสนเทศของหน่วยงาน โดยส่วนใหญ่จะเชื่อมต่อผ่านระบบเครือข่ายไร้สาย (Wi-Fi) ของหน่วยงานด้วยกระบวนการตรวจยืนยันผู้ใช้งานที่กำหนดไว้ และอุปกรณ์ BYOD นั้น เมื่อมีการเชื่อมต่อเข้ากับระบบระบบคอมพิวเตอร์และเครือข่ายสารสนเทศของสำนักแล้ว ในครั้งต่อๆ ไป มักมีการตั้งค่าให้สามารถเชื่อมต่อเองโดยอัตโนมัติ ทำให้เกิดความเสี่ยงที่อุปกรณ์ BYOD จะสูญหาย และอาจถูกนำมาใช้เป็นเครื่องมือในการเชื่อมต่อเข้ากับระบบเครือข่ายของหน่วยงานได้ รวมถึงการโจรกรรมค่าสำคัญในตัวอุปกรณ์ BYOD เช่น ชื่อบัญชีผู้ใช้งานและรหัสผ่าน รหัส Wi-Fi ฯลฯ เพื่อนำไปใช้ในการเชื่อมต่อเข้าสู่ระบบของหน่วยงาน แนวทางในการ

ป้องกันคือ การตั้งค่าการเชื่อมต่อโดยไม่ให้อุปกรณ์จดจำค่าต่างๆ และทำการเชื่อมต่อโดยอัตโนมัติ และยังควรนำระบบการพิสูจน์ตัวตนแบบพหุปัจจัย (Multi-Factor Authentication) มาใช้ในการตรวจยืนยันตัวตนของผู้ใช้งานด้วย เช่น รหัสแบบ One-Time Password (OTP) นอกจากนี้ หน่วยงานอาจนำระบบการลงทะเบียนอุปกรณ์ที่จะมาเชื่อมต่อกับระบบเครือข่ายสารสนเทศของหน่วยงานมาใช้ เพื่อขึ้นทะเบียนหมายเลขเฉพาะประจำตัวของอุปกรณ์ (MAC Address) BYOD ของผู้นำมาใช้ในการปฏิบัติงาน และอนุญาตการเชื่อมต่อเฉพาะอุปกรณ์ที่ลงทะเบียนอย่างถูกต้องเท่านั้น

นอกจากนี้ สิ่งที่ต้องระมัดระวังเพิ่มเติมคือ การที่อุปกรณ์ BYOD อาจเป็นพาหะนำไวรัสหรือมัลแวร์อันตรายแพร่กระจายไปสู่ระบบคอมพิวเตอร์และเครือข่ายสารสนเทศของหน่วยงานด้วย โดยแนวทางในการป้องกันคือ การใช้อุปกรณ์ BYOD อย่างระมัดระวังเช่นเดียวกับการใช้อุปกรณ์คอมพิวเตอร์ของหน่วยงาน และหลีกเลี่ยงพฤติกรรมการใช้งานอันจะนำไปสู่การติดไวรัสหรือมัลแวร์อันตราย

๑.๖.๒ การใช้ข้อมูลในระบบสารสนเทศหน่วยงานผ่านอุปกรณ์ BYOD

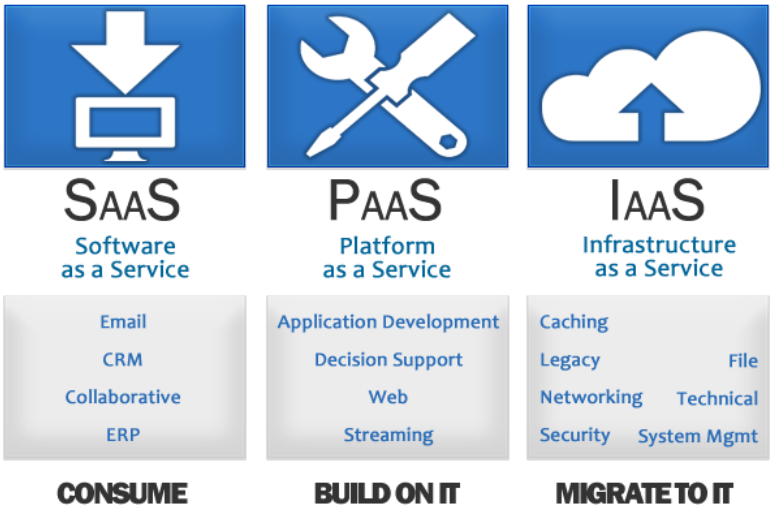
อุปกรณ์ BYOD ที่นำมาใช้ร่วมในหน่วยงาน มักจะมีการเรียกใช้ข้อมูลจากระบบสารสนเทศของสำนักด้วยเสมอ ทำให้ข้อมูลถูกถ่ายโอนไปยังตัวอุปกรณ์ BYOD ด้วย เช่น อีเมล และไฟล์เอกสารต่างๆ ซึ่งข้อมูลดังกล่าวอาจมีการรั่วไหลหากการรักษาความปลอดภัยบนตัวอุปกรณ์ BYOD ไม่ดีพอ ทำให้มีความเสี่ยงต่อการรั่วไหลของข้อมูลสำคัญของหน่วยงานได้ แนวทางในการป้องกันคือ การใช้อุปกรณ์ BYOD อย่างระมัดระวังเช่นเดียวกับการใช้อุปกรณ์คอมพิวเตอร์ของหน่วยงาน และหลีกเลี่ยงพฤติกรรมการใช้งานอันจะนำไปสู่การติดไวรัสหรือมัลแวร์อันตราย และการตั้งค่า PIN Code หรือรหัสผ่าน ในการเรียกใช้งานอุปกรณ์ BYOD หรือการเข้ารหัสไฟล์ข้อมูลในตัวอุปกรณ์ BYOD เพื่อความปลอดภัยของข้อมูล เป็นต้น

๑.๗ การใช้บริการจัดเก็บข้อมูลบน Cloud Services กับการรักษาความปลอดภัย

หน่วยงานสมัยใหม่ นอกจากจะลงทุนด้านระบบคอมพิวเตอร์และเครือข่ายสารสนเทศเองแล้ว ยังสามารถใช้บริการประเภทต่างๆ ของระบบ Cloud Services ได้อีกด้วย เพราะเป็นการเช่าใช้บริการประเภทที่ตรงต่อความต้องการของหน่วยงานด้วยการชำระค่าบริการตามที่ใช้งาน โดยไม่ต้องลงทุนสร้างโครงสร้างพื้นฐานตลอดจน Hardware/Software ของหน่วยงานเอง

รูปแบบการให้บริการของระบบ Cloud Services แบ่งออกเป็น ๓ แบบ (ภาพที่ ๑.๓๘) ได้แก่ บริการด้านซอฟต์แวร์ (Software as a Service : SAAS) บริการด้านแพลตฟอร์ม (Platform as a Service : PAAS) และบริการด้านโครงสร้างพื้นฐาน (Infrastructure as a Service : IAAS)

หนึ่งในบริการแบบ Cloud Services รูปแบบ SAAS ที่หน่วยงานสมัยใหม่นิยมใช้งานกันมากที่สุด ได้แก่ “**การเก็บข้อมูลแบบก้อนเมฆ** (Cloud Storage)” หรือการฝากเก็บไฟล์ข้อมูลเอาไว้บนอินเทอร์เน็ต โดยที่ผู้ใช้งานสามารถเข้าถึงข้อมูลที่ฝากเอาไว้ได้ตลอดเวลา จากเครื่องคอมพิวเตอร์ (Desktop, Notebook) สมาร์ทโฟน หรือแท็บเล็ต จากทุกที่ที่สามารถเชื่อมต่อกับอินเทอร์เน็ตได้



ภาพที่ ๑.๓๘ บริการรูปแบบต่างๆ ของ Cloud Services

ในด้านของการใช้งานแล้ว ประโยชน์สำคัญอย่างยิ่งของ Cloud Storage ก็คือ การที่ข้อมูลต่างๆ ซึ่งฝากอยู่ในระบบ Cloud Storage นั้น จะถูก “ซิงค์ (Sync)” ลงในเครื่องคอมพิวเตอร์ตลอดจนอุปกรณ์ประเภทสมาร์ทโฟนและแท็บเล็ตที่เราลงโปรแกรม (หรือ Application) ของผู้ให้บริการจัดเก็บข้อมูลดังกล่าวไว้ด้วย ตลอดเวลา (ต้องใช้ ID: Username, Password เดียวกัน) ซึ่งหมายถึงว่าหากมีการเปลี่ยนแปลง เช่น มีการแก้ไข ปรับปรุง เพิ่มเติม หรือลบข้อมูลใดๆ จากอุปกรณ์ใดๆ (คอมพิวเตอร์, สมาร์ทโฟน, แท็บเล็ต) ที่กำลังเชื่อมต่อและเข้าถึงข้อมูลนั้นๆ ขึ้น การเปลี่ยนแปลงนั้นก็จะถูกซิงค์และอัพเดทตัวเอง (Sync & Update) แล้วแสดงผลความเป็นปัจจุบันของข้อมูลที่หน้าจอ Interface ของโปรแกรมที่เราใช้งานทันที ในทุกอุปกรณ์ที่มีการเปิดใช้งานโปรแกรมอยู่ (ภาพที่ ๑.๓๙)

ภาพที่ ๑.๓๙ การ Sync & Update ข้อมูลในระบบ Cloud Storage

การใช้งานที่ตอบสนองต่อรูปแบบการทำงานของผู้ปฏิบัติงานในหน่วยงานที่ต้องมีการเคลื่อนที่อยู่ตลอดเวลา (Mobility) โดยไม่จำเป็นที่จะต้องนำอุปกรณ์บันทึกข้อมูลสำรอง เช่น ฮาร์ดดิสก์แบบพกพา หรืออุปกรณ์บันทึกข้อมูลประเภทแฟลชไดรฟ์ (Flash Drive) ติดตัวไปด้วยนี้ เป็นจุดเด่นที่สำคัญซึ่งสามารถดึงดูดความสนใจของผู้ใช้งาน และที่สำคัญอีกอย่างหนึ่งก็คือ ปัญหาการลืมบันทึกไฟล์ที่อัพเดทใช้งานล่าสุดลงในอุปกรณ์บันทึกข้อมูลแบบพกพาต่างๆ ก็จะหมดไปด้วย (เมื่อผู้ใช้งานเชื่อมต่ออินเทอร์เน็ต จะสามารถเรียกไฟล์ที่อัพเดทล่าสุดใช้งานได้ทันที)

ปัจจุบันมีผู้ให้บริการ Cloud Storage ที่ได้รับความนิยมอยู่หลายแห่ง (ภาพที่ ๑.๔๐) มีทั้งประเภทที่เปิดให้บริการโดยไม่เสียค่าใช้จ่าย (พื้นที่เก็บบันทึกข้อมูลมีจำกัด ฯลฯ) และประเภทที่เสียค่าใช้จ่าย (พื้นที่เก็บข้อมูลมีขนาดใหญ่ถึงใหญ่มากแยกตาม Package) เช่น iCloud, box, Google Drive, SkyDrive และ Dropbox เป็นต้น โดยผู้ให้บริการ Cloud Storage แต่ละแห่ง จะมีเงื่อนไขการให้บริการที่มีความแตกต่างกัน และอาจมีหน้าตาของ Interface การใช้งานที่มีข้อดีและข้อเสียเฉพาะตัวแตกต่างกันไป อย่างไรก็ตาม ปัจจุบันพบว่ามีจำนวนผู้ใช้งานในการเก็บข้อมูลไว้บน Cloud Storage เพิ่มขึ้นเป็นลำดับ โดยเฉพาะอย่างยิ่ง การเลือกใช้บริการที่ไม่มีค่าใช้จ่าย แม้ว่าพื้นที่ที่ได้รับในการเก็บข้อมูลจะมีขนาดที่จำกัดก็ตาม เช่น iCloud 5 GB, box, Google Drive 5 GB, SkyDrive 7 GB และ Dropbox 2 GB เป็นต้น ทั้งนี้ บางผู้ให้บริการ จะเพิ่มขนาดของพื้นที่จัดเก็บข้อมูลให้อีกหากมีการแนะนำเพื่อนฝูงที่รู้จักให้เข้ามาใช้บริการของ Cloud Storage นั้นๆ ด้วย

ภาพที่ ๑.๔๐ ตัวอย่างผู้ให้บริการ Cloud Storage

การใช้งาน Cloud Storage ยังมีข้อดีอีกข้อหนึ่งที่น่าสนใจเป็นอย่างยิ่งคือ “การใช้งานร่วมเป็นกลุ่ม” ซึ่งเป็นการร่วมแชร์โฟลเดอร์ที่จัดเก็บไฟล์ข้อมูลที่ต้องมีการใช้งานร่วมกันระหว่างบุคคลภายในกลุ่ม ยกตัวอย่างเช่น สมชายสมัครใช้บริการ Cloud Storage จากผู้ให้บริการแห่งหนึ่ง และสร้าง

โฟลเดอร์ที่ชื่อ “ข้อมูลส่วนตัว” กับ โฟลเดอร์ที่ชื่อ “งานพัฒนาองค์กร” โดยโฟลเดอร์แรกเป็นโฟลเดอร์ที่ใช้จัดเก็บข้อมูลต่างที่ใช้ส่วนบุคคลของสมชาย และโฟลเดอร์ที่สองเป็นโฟลเดอร์ที่ใช้รวบรวมและแชร์ข้อมูลที่เกี่ยวข้องกับงานพัฒนาองค์กรกับสมาชิกทุกคนในหน่วยงาน โดยมุ่งหวังที่จะให้สมาชิกแต่ละคนในทีมทำการอัพโหลดไฟล์ข้อมูล (จากคอมพิวเตอร์, สมาร์ทโฟน, แท็บเล็ต ของสมาชิกแต่ละคน) ในส่วนที่ตัวเองรับผิดชอบ ขึ้นไปเก็บไว้ใน Cloud Storage ในโฟลเดอร์ที่ชื่อ “งานพัฒนาองค์กร” โดยที่ข้อมูลต่างๆ ที่สมาชิกแต่ละคนอัพโหลดขึ้นไปจัดเก็บนั้น จะถูกจัดเก็บรวมกันอยู่ที่แหล่งเก็บข้อมูลที่เป็นศูนย์กลาง (Centralized Storage) ซึ่งสมาชิกทุกคนสามารถเรียกดูข้อมูลทั้งหมดได้ตลอดเวลา เนื่องจากข้อมูลที่มีการอัพโหลดขึ้นไปใหม่นั้น จะถูกซิงค์และอัพเดท (Sync & Update) ในหน้าจอ Interface โปรแกรม ใน คอมพิวเตอร์, สมาร์ทโฟน และ แท็บเล็ต ของสมาชิกคนอื่นๆ ในกลุ่มด้วยทันทีที่มีการอัพโหลดข้อมูล ทั้งนี้ แหล่งเก็บข้อมูลบน Cloud Storage แบบรวมศูนย์นี้ รองรับต่อ การลบ, แก้ไข, เพิ่มเติม ฯลฯ ข้อมูลด้วย เช่น เมื่อสมาชิกคนใดเปิดไฟล์ขึ้นมาแก้ไขแล้วบันทึกจัดเก็บใหม่ สมาชิกคนอื่นๆ ก็จะได้รับไฟล์ที่ถูกปรับปรุงล่าสุดไปพร้อมๆ กันด้วยเสมอ (ภาพที่ ๑.๔๑)

ประโยชน์ที่จะได้รับนอกเหนือจากการมีแหล่งเก็บข้อมูลที่เป็นศูนย์กลางซึ่งสมาชิกทุกคนสามารถเชื่อมต่อและเข้าถึงข้อมูลที่อัพเดทเป็นปัจจุบันได้ตลอดเวลาผ่านการใช้งานจากเครื่องคอมพิวเตอร์ (Desktop, Notebook) หรืออุปกรณ์สมาร์ทโฟนและแท็บเล็ต ได้อย่างสะดวกแล้ว ในกรณีที่มีการประชุมทีมงาน ยังสามารถช่วยลดการใช้กระดาษพิมพ์ข้อมูลแจกผู้ที่เกี่ยวข้อง และยังช่วยให้สมาชิกทุกคนสามารถเรียกดูข้อมูลต่างๆ เช่น ไฟล์ข้อมูลนำเสนอ (ไฟล์ PowerPoint) จากหน้าจอสมาร์ทโฟน หรือแท็บเล็ตของตัวเองได้โดยตรง เมื่ออยู่ในห้องประชุม (เช่น อยู่ไกลจากจอภาพ หรือกรณีตัวอักษรบนสไลด์มีขนาดเล็ก ฯลฯ) ได้เป็นอย่างดีอีกด้วย

ภาพที่ ๑.๔๑ การแชร์ข้อมูลใน Cloud Storage

ประโยชน์ในทางอ้อมอีกอย่างหนึ่งที่น่าสนใจ ได้แก่ การเก็บบันทึกการประชุมต่างๆ ของทีมงานเอาไว้ในโฟลเดอร์ที่แชร์ข้อมูลกัน เพื่อให้สมาชิกสามารถที่จะเรียกดูข้อมูลสำคัญที่เคยประชุมกันไว้ ย้อนหลังได้ตลอดเวลาอีกด้วย (ในโฟลเดอร์ “งานพัฒนาองค์กร” ซึ่งเป็นโฟลเดอร์หลัก สามารถสร้างโฟลเดอร์ย่อยที่ต้องการได้เอง เช่น สร้างโฟลเดอร์ “ข้อมูลนำเสนอ” และโฟลเดอร์ “บันทึกการประชุม” เป็นต้น) (ภาพที่ ๑.๔๒)

ภาพที่ ๑.๔๒ ตัวอย่างการเพิ่มข้อมูลใช้ร่วมเป็นโฟลเดอร์ย่อยลงใน Cloud Storage

การใช้บริการจัดเก็บข้อมูลแบบ Cloud Storage ให้ความสะดวกในการจัดการข้อมูลของหน่วยงาน แต่สิ่งสำคัญที่ไม่ควรมองข้าม คือการรักษาความปลอดภัยในด้านของการรักษาความลับของข้อมูล (Data Confidentiality) ที่มีการแชร์บน Cloud Starage และการรักษาความเป็นส่วนตัวของผู้ใช้งาน (Privacy) กล่าวคือ จะต้องระมัดระวังไม่แชร์ข้อมูลสำคัญยิ่ง/ข้อมูลลับ/ข้อมูลที่ละเอียดอ่อนของหน่วยงานลงในระบบ เนื่องจากแหล่งเก็บข้อมูลจะเป็นของผู้ให้บริการ Cloud Storage ซึ่งในทางปฏิบัติสามารถเข้าถึงข้อมูลได้ หรือต้องมีการนำระบบการเข้ารหัสข้อมูล (Data Encryption) มาใช้ก่อนจัดเก็บลงในระบบ Cloud Starage เพื่อเป็นการรักษาความลับของเนื้อข้อมูล นอกจากนี้ ยังต้องระมัดระวังอนุญาตให้เฉพาะผู้ที่เกี่ยวข้องสามารถเรียกดูข้อมูลได้ด้วย เพื่อป้องกันการเข้าถึงข้อมูลจากผู้ที่ไม่มีความเกี่ยวข้อง

บทที่ ๒
เทคโนโลยีที่ด้านความปลอดภัยที่สำคัญ

เทคโนโลยีด้านความปลอดภัยที่สำคัญที่ควรทราบและทำความเข้าใจ ได้แก่ การใช้การพิสูจน์ยืนยันตัวตนแบบพหุปัจจัย (Multi-factor Authentication) การลงลายมือชื่อดิจิทัล (Digital Signature) และเทคโนโลยี BLOCKCHAIN ดังนี้

๒.๑ การพิสูจน์ยืนยันตัวตนแบบพหุปัจจัย (Multi-factor Authentication)

นับตั้งแต่อดีต การทำธุรกรรมสำคัญส่วนบุคคลกับองค์กรภาครัฐหรือภาคเอกชนประเภทธุรกิจหรือการให้บริการ จะต้องปฏิบัติผ่านตัวตนจริงของบุคคลนั้นเสมอ เพื่อเป็นการยืนยันถึงความถูกต้องในความเป็นเจ้าของการทำธุรกรรม ปัจจุบันรูปแบบการทำธุรกรรมสามารถปฏิบัติได้อย่างสะดวกผ่านระบบเครือข่ายแบบออนไลน์จากทุกที่ที่มีการเชื่อมต่อเข้ากับตัวระบบบริการ และจากการที่รูปแบบการทำธุรกรรมได้เปลี่ยนแปลงไปอยู่บนพื้นฐานของการให้บริการแบบไม่จำกัดเวลาและสถานที่ ทำให้หนึ่งในปัญหาที่ตามมาก็คือ “**การระบุตัวตนและการพิสูจน์เพื่อยืนยันตัวตน**” ของผู้ทำธุรกรรม ด้วยวิธีที่ทำให้แน่ใจได้ว่า ผู้ทำธุรกรรมนั้นเป็นตัวตนที่แท้จริง มิใช่ถูกลักลอบกระทำโดยบุคคลอื่นที่ไม่ประสงค์ดี

การยืนยันตัวตนของผู้ใช้งานในหน่วยงานก็เช่นเดียวกัน โดยเฉพาะเมื่อมีการนำอุปกรณ์ BYOD ซึ่งมีความสะดวกสามารถพกพาได้มาใช้ร่วมกับงานหน่วยงาน จำเป็นที่จะต้องมีกระบวนการในการตรวจสอบเพื่อยืนยันถึงตัวตนของผู้ใช้งานที่มีความปลอดภัยและเชื่อถือได้ ทั้งนี้ กระบวนการพิสูจน์ยืนยันตัวตนจะตอบสนองต่อความปลอดภัยขั้นแรกในการเข้าถึงระบบคอมพิวเตอร์และเครือข่ายสารสนเทศของหน่วยงาน ก่อนที่จะมีการเรียกใช้ทรัพยากรสารสนเทศของหน่วยงาน และการยืนยันตัวตนในขั้นตอนการเรียกใช้ทรัพยากรสารสนเทศของหน่วยงาน เช่น อีเมล และไฟล์ข้อมูลจากแหล่งรวมที่มีการแชร์ เป็นต้น

รูปแบบที่เข้าใจได้ง่ายที่สุด ได้แก่ การป้อนค่าผู้ใช้งานและรหัสผ่าน (Username & Password) เพื่อ Log-in เข้าสู่เครื่องคอมพิวเตอร์ แล้วทำการรับ-ส่งอีเมล ซึ่งผู้ใช้บริการจะต้องกรอกชื่อบัญชีผู้ใช้ (E-mail Address) ลงไป พร้อมกับใส่รหัสผ่าน (Password) สำหรับชื่อบัญชีอีเมลลงไปให้ถูกต้อง เพื่อเริ่มใช้บริการอีเมลดังกล่าว ตรงนี้ มีสองขั้นตอนหลักที่สำคัญ ได้แก่ “การกรอกชื่อบัญชีอีเมล” และ “การใส่รหัสผ่านสำหรับชื่อบัญชีอีเมล” ซึ่งการกรอกชื่อบัญชีอีเมลจะหมายถึงการระบุตัวตนของผู้ใช้งานหรือ User Identification โดยมีชื่อบัญชีอีเมลเป็น Identity และการใส่รหัสผ่านสำหรับชื่อบัญชีอีเมลจะหมายถึงการยืนยันตัวตนของผู้ใช้งาน หรือ User Authentication ว่าผู้ที่กำลังเรียกใช้งานบริการอีเมลอยู่นั้นเป็นตัวตนที่แท้จริงของผู้ใช้ชื่อบัญชีอีเมลนั้น ผ่านกระบวนการในการตรวจพิสูจน์ (Verification) ว่ารหัสผ่านดังกล่าวเป็นของชื่อบัญชีนั้นถูกต้องหรือไม่ ซึ่งหลังจากตรวจพิสูจน์และยืนยันตัวตนแล้ว ผู้ใช้งานจะสามารถเรียกใช้บริการประเภทใดหรือสามารถเข้าถึงข้อมูลชนิดใดได้บ้าง จะเป็นเรื่องของกระบวนการให้สิทธิ์อนุญาต หรือ Authorization จากผู้รับผิดชอบดูแลระบบของหน่วยงาน

จะเห็นได้ว่าขั้นตอนทั้งหมดในการตรวจพิสูจน์เพื่อยืนยันตัวตน (User Identification-(Verification)-Authentication) เป็นขั้นตอน Access ที่สำคัญยิ่งในการร้องขอเพื่อทำธุรกรรมหรือเรียกใช้บริการ ผ่านเครือข่ายอินเทอร์เน็ต เพราะตัวผู้ใช้งานสามารถที่จะขอทำธุรกรรมหรือเรียกใช้งานบริการจากที่ใดก็ได้ ดังนั้นการตรวจพิสูจน์เพื่อยืนยันตัวตนของผู้ใช้งานจึงเป็นกระบวนการที่ต้องปฏิบัติได้อย่างถูกต้องและปลอดภัยเสมอ โดยปัจจัยที่ใช้ในการตรวจพิสูจน์ยืนยันตัวตนแบ่งออกเป็น ๓ ประเภท ดังนี้

๒.๑.๑ สิ่งที่ผู้ใช้ทราบ (Something you know : Knowledge Factors)

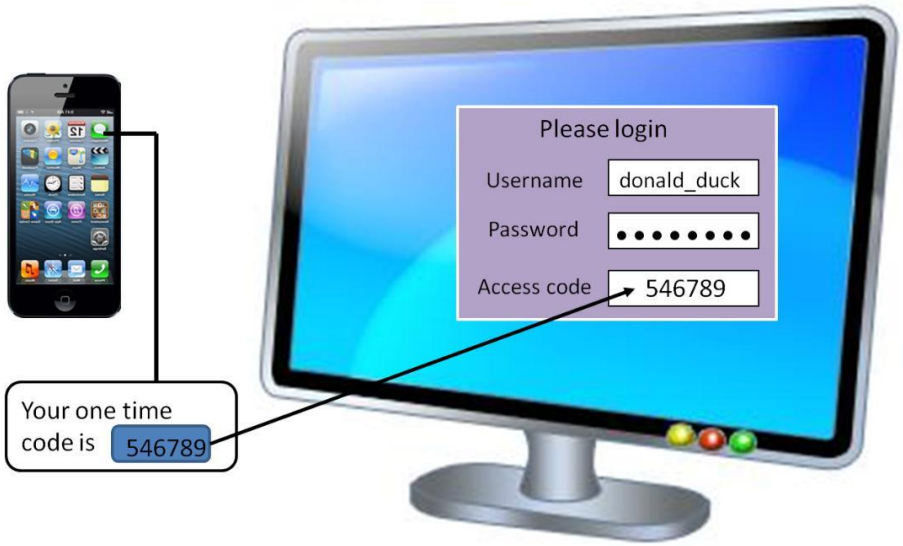
ตัวอย่างที่เข้าใจง่ายและใกล้ตัวที่สุด ได้แก่ การที่นำบัตร ATM ไปกดเงินที่ตู้ ให้บริการซึ่งตู้ ATM จะไม่ทราบว่าผู้ใช้บริการเป็นใคร และขั้นตอนแรกในกระบวนการดังกล่าวได้แก่ การนำบัตร ATM ใส่เข้าไปในช่องรับบัตร ซึ่งตู้ ATM จะอ่านข้อมูลที่บันทึกอยู่ในบัตรเพื่อให้ทราบว่าเป็นบัตรของใคร (User Identification โดยมีตัวบัตรเป็น identity) เมื่อทราบข้อมูลดังกล่าวแล้ว ขั้นตอนต่อไปคือ การตรวจพิสูจน์เพื่อยืนยันว่าผู้ที่ใส่บัตรเข้ามานั้นเป็นเจ้าของบัตรจริงหรือไม่ ซึ่งโดยปกติแล้วเครื่อง ATM จะถามรหัสตัวเลขลับ (PIN Number) ๔ หลักหรือ ๖ หลัก ที่ทางธนาคารผู้ออกบัตรได้มอบให้กับผู้ใช้บริการบัตร ATM ในตอนแรกหรือรหัสตัวเลขลับ ๔ หลักหรือ ๖ หลักที่ผู้ใช้บัตรตั้งเองขึ้นมาใหม่ (โดยจะต้องใส่รหัสตัวเลขลับ ๔ หลักหรือ ๖ หลักที่ได้รับจากทางธนาคารก่อน จึงจะสามารถเปลี่ยนรหัสลับใหม่ได้) ซึ่งข้อมูลรหัสตัวเลขลับตรงนี้ ถือเป็นข้อมูลประเภท **“สิ่งที่ผู้ใช้ทราบ** (Something you know)” ซึ่งเป็นข้อมูลจำพวก Knowledge Factors บนพื้นฐานที่ว่า ผู้ใช้บัตรมีหน้าที่ในการเก็บรหัสตัวเลขลับนั้นไว้ด้วยวิธีที่ปลอดภัยโดยไม่ให้ผู้อื่นล่วงรู้ ดังนั้น การที่มีผู้ใส่บัตร ATM พร้อมกดรหัสตัวเลขลับ ๔ หลักหรือ ๖ หลักได้อย่างถูกต้อง จึงน่าจะสามารถพิสูจน์ยืนยันได้ว่าผู้นั้นเป็นเจ้าของบัตรตัวจริง อย่างไรก็ตาม ในการใช้บริการตู้ ATM นั้น ส่วนใหญ่เป็นการใช้บริการในพื้นที่ที่เปิดเผยและมีกล้องวงจรปิดติดตั้งอยู่ การพิสูจน์ยืนยันตัวตนด้วยรหัสตัวเลขลับ ๔ หลักหรือ ๖ หลักเพียงอย่างเดียวจึงเป็นที่นิยมปฏิบัติ แต่หากเป็นการทำธุรกรรมหรือการเรียกใช้บริการต่างๆ ที่มีความสำคัญสูงๆ จากที่ใดก็ได้ที่มีการเชื่อมต่อกับอินเทอร์เน็ต กระบวนการพิสูจน์เพื่อยืนยันตัวตนจะต้องมีวิธีและขั้นตอนที่สามารถให้ความถูกต้องและปลอดภัยที่มากยิ่งขึ้น เพราะจะไม่มีผู้ใดทราบว่าผู้ที่ทำธุรกรรมหรือเรียกใช้บริการอยู่นั้นเป็นใคร ใช่ตัวตนที่แท้จริงหรือไม่

๒.๑.๒ สิ่งที่ผู้ใช้มี (Something you have : Possession factors)

การนำ **“สิ่งที่ผู้ใช้มี”** มาใช้ร่วมในกระบวนการตรวจพิสูจน์เพื่อยืนยันตัวตนนั้นแบ่งออกเป็น ๒ ชนิดหลักๆ ได้แก่ แบบรหัส (Code Type) และแบบวัตถุทางกายภาพ (Physical Type) ดังนี้

๒.๑.๒.๑ แบบรหัส (Code Type) ตัวอย่างของการนำ **“สิ่งที่ผู้ใช้มี”** แบบรหัส (Code Type) เข้ามาใช้ร่วมในกระบวนการตรวจพิสูจน์เพื่อยืนยันตัวตนที่เข้าใจได้โดยง่าย ได้แก่ การส่งรหัส OTP (One Time Password) เข้าไปที่โทรศัพท์มือถือของผู้ใช้งานในลักษณะของ SMS หรือส่งไปที่บัญชีอีเมลของผู้ใช้งานในลักษณะของข้อความเมล (ภาพที่ ๒.๑) เพื่อให้ผู้ที่ทำธุรกรรมหรือเรียกใช้บริการบนอินเทอร์เน็ตกรอกรหัส (Code) ที่ได้รับนั้นเพิ่มเติมลงไป ควบคู่กับชื่อบัญชีผู้ใช้งาน (username) และรหัสผ่าน (Password) ปกติ ทั้งนี้ ผู้ใช้บริการจะเป็นผู้แจ้งหมายเลขโทรศัพท์มือถือดังกล่าวหรือชื่อบัญชีอีเมลสำหรับรับรหัส OTP ให้แก่ผู้ให้บริการทราบล่วงหน้าในขั้นตอนของการ

ลงทะเบียนใช้งาน โดยจะอนุมานว่าผู้ที่ถือโทรศัพท์หรือผู้ที่สามารถเปิดอีเมลเพื่อรับและอ่านค่า OTP ได้นั้น เป็นตัวตนที่แท้จริงของผู้ใช้บริการ ทั้งนี้และทั้งนั้น ความผิดพลาดจะเกิดขึ้นได้ในกรณีที่ชื่อบัญชีของผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตกอยู่ในมือของผู้อื่น (ที่ไม่ประสงค์ดี) พร้อมกับเครื่องโทรศัพท์มือถือ หรือชื่อบัญชีอีเมลและรหัสผ่านอีเมลของผู้ใช้งานก็ตกอยู่ในมือของผู้นั้น (ผู้นั้นสามารถเปิดเข้าไปอ่านรหัส OTP ได้) ซึ่งเป็นไปได้ยากในทางปฏิบัติ



ภาพที่ ๒.๑ ปัจจัยตรวจพิสูจน์ยืนยันด้วย “สิ่งที่ผู้ใช้มี” แบบรหัส (Code Type)

๒.๑.๒.๒ แบบวัตถุทางกายภาพ (Physical Type) เป็นการนำ “Token” ซึ่งเป็นอุปกรณ์พิเศษที่มีชุดข้อมูลลับเฉพาะตัวบางอย่างบันทึกไว้ภายใน (ข้อมูลแตกต่างไปตามผู้ใช้งาน) ทั้งแบบ Hardware และแบบ Software (ภาพที่ ๒.๒) (Token จะต้องไม่สามารถถูก Copy ได้ง่าย เช่น มีการนำเทคโนโลยีการเข้ารหัสที่ให้ความปลอดภัยสูงในระดับสากลมาใช้ร่วม) เช่น Authentication Token, USB Token, Cryptographic Token, Virtual Token (ทั้งแบบต้องต่อเชื่อมกับ Hardware และแบบไม่ต่อเชื่อมกับ Hardware เช่น RFID Type และ Bluetooth Type) เข้ามาใช้ร่วมในกระบวนการตรวจพิสูจน์เพื่อยืนยันตัวตน

โดยผู้ขอใช้บริการจะได้รับแจกตัว Token จากผู้ให้บริการ เพื่อเก็บไว้เป็นการส่วนตัว และจะต้องนำมาใช้กับระบบควบคู่ไปกับชื่อบัญชีผู้ใช้งาน (username) และรหัสผ่าน (Password) ทุกครั้งที่มีการใช้บริการ ทั้งนี้ ชุดข้อมูลลับเฉพาะที่ถูกบันทึกอยู่ใน Token เหล่านั้นจะถูกอ่านค่าเพื่อนำไปตรวจพิสูจน์ยืนยันตัวตนของผู้ใช้งานจากอุปกรณ์ในการอ่านค่าแบบต่างๆ ทั้งแบบเชื่อมต่อและแบบไม่เชื่อมต่อ หรือชุดของรหัส (Code) ซึ่งประมวลขึ้นโดยอุปกรณ์ Token ในแต่ละครั้งที่ใช้งานจะถูกนำไปป้อนค่าเข้าสู่ระบบควบคู่ไปด้วย เช่นเดียวกัน ความผิดพลาดจะเกิดขึ้นได้ในกรณีที่ชื่อบัญชีของผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตกอยู่ในมือของผู้อื่น (ที่ไม่ประสงค์ดี) พร้อมกับอุปกรณ์ Token ของตัวเองก็ตกอยู่ในมือของผู้นั้น ซึ่งเป็นไปได้ยากขึ้นในทางปฏิบัติ

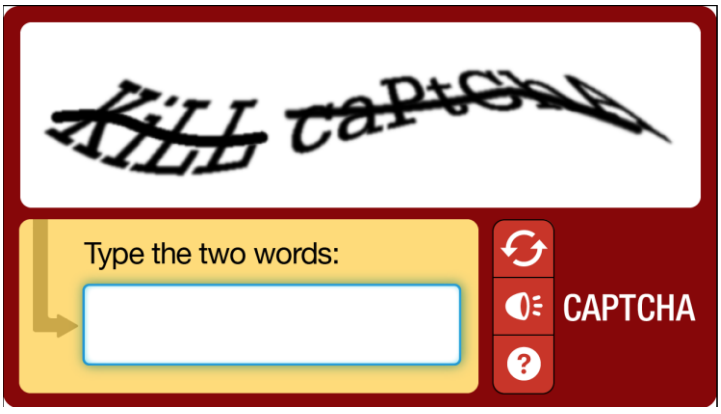
ภาพที่ ๒.๒ ปัจจัยตรวจพิสูจน์ยืนยันด้วย “สิ่งที่ผู้ใช้มี” แบบวัตถุทางกายภาพ (Physical Type)

๒.๑.๓ สิ่งที่ผู้ใช้เป็น (Something you are : Inherence factors)

การนำ “**สิ่งที่ผู้ใช้เป็น**” มาใช้ร่วมในกระบวนการตรวจพิสูจน์เพื่อยืนยันตัวตนนั้น เป็นลักษณะของการตรวจสอบทางด้านกายภาพของตัวบุคคลจากอัตลักษณ์ของบุคคลที่เป็นข้อมูลประเภท Biometric เป็นหลัก (ภาพที่ ๒.๓) เช่น การตรวจสอบลายนิ้วมือ (Fingerprint) การตรวจสอบม่านตา (Retinal) การตรวจสอบเสียง (Voice) การตรวจสอบลายเซ็น (Signature) หรือการตรวจสอบทางด้านกายภาพจากพฤติกรรมที่บุคคลปฏิบัติ เช่น จังหวะห้วงเวลาหรือความเร็วของการพิมพ์ตัวอักษรลงในคอมพิวเตอร์ (keystroke Timing) โดยความผิดพลาดจะเกิดขึ้นได้ในกรณีที่ชื่อบัญชีของผู้ใช้งาน (Username) และรหัสผ่าน (Password) ตกอยู่ในมือของผู้อื่น (ที่ไม่ประสงค์ดี) พร้อมๆ กับตัวผู้ใช้งานเองก็ตกอยู่ในการควบคุมของผู้นั้น (ถูกบังคับให้สแกนลายนิ้วมือ, ม่านตา หรือถูกบังคับให้พูดออกเสียง หรือถูกบังคับให้พิมพ์ข้อความใดๆ ในการตรวจสอบ Keystroke Time) ซึ่งเป็นไปได้ยากยิ่งขึ้นในทางปฏิบัติ

ภาพที่ ๒.๓ ปัจจัยตรวจพิสูจน์ยืนยันด้วย “สิ่งที่ผู้ใช้เป็น”

การตรวจสอบด้วย “**สิ่งที่ผู้ใช้เป็น**” นั้น ในหลายบริการ ผู้ให้บริการเพียงแต่ต้องการตรวจพิสูจน์เพื่อยืนยันว่าผู้ใช้บริการนั้นเป็น “มนุษย์ (Human)” ไม่ใช่เป็น “โปรแกรมคอมพิวเตอร์ที่ทำงานอัตโนมัติ” ด้วยการนำวิธีการของ CAPTCHA มาใช้ (ภาพที่ ๒.๔) เพื่อให้ผู้ใช้งาน (ที่เป็นมนุษย์) อ่านค่าของตัวชุดอักษรหรือตัวเลขจากภาพที่กำหนด แล้วกรอกค่าที่อ่านได้ลงไป โดยหากใส่ค่าที่ถูกต้องก็จะอนุมานว่าผู้ใช้งานนั้นเป็นมนุษย์จริงๆ



ภาพที่ ๒.๔ การนำ CAPTCHA มาใช้ร่วมกับ “สิ่งที่ผู้ใช้เป็น”

จากที่กล่าวมา จะเห็นได้ว่าการนำปัจจัยหรือองค์ประกอบที่มากกว่าหนึ่งอย่างมาใช้ควบคู่กันในระบบการตรวจพิสูจน์เพื่อยืนยันตัวตนของผู้ใช้งาน (Multi-factor User Authentication) จะทำให้สามารถที่จะรักษาความปลอดภัยในขั้นตอนของการ Access เข้าสู่ระบบได้อย่างมีประสิทธิผลที่สูงขึ้น

โดยเฉพาะในการทำธุรกรรมหรือเรียกใช้บริการที่มีความสำคัญสูงผ่านเครือข่ายอินเทอร์เน็ต ที่ผู้ร้องขอสามารถร้องขอการขอรับบริการจากที่ใดก็ได้ที่สามารถเชื่อมต่อกับระบบอินเทอร์เน็ตได้ ซึ่งในทางปฏิบัติโดยทั่วไปแล้ว มักพบการนำปัจจัยหรือองค์ประกอบสองอย่าง (Two-factor Authentication) มาใช้ในกระบวนการดังกล่าว เช่น (๑) การใช้ชื่อบัญชีผู้ใช้งาน (Username) ควบคู่ไปกับการตรวจสอบรหัสผ่าน (Password) และอุปกรณ์ Token ที่แจกจ่ายให้กับผู้ใช้งาน หรือ (๒) การใช้ชื่อบัญชีผู้ใช้งาน (Username) ควบคู่ไปกับการตรวจสอบรหัสผ่าน (Password) และรหัส OTP ที่ส่งไปยังโทรศัพท์มือถือหรือส่งไปที่บัญชีอีเมลของผู้ใช้งาน หรือ (๓) การใช้ชื่อบัญชีผู้ใช้งาน (Username) ควบคู่ไปกับการตรวจสอบรหัสผ่าน (Password) และข้อมูลประเภท Biometric (Fingerprint, Retina, Voice, Signature, Keystroke Timing) ของผู้ใช้งาน

๒.๒ การลงลายมือชื่อดิจิทัล (Digital Signature)

หน่วยงานสมัยใหม่มีแนวโน้มที่จะบริหารจัดการแบบเบ็ดเสร็จบนพื้นฐานของระบบดิจิทัล ซึ่งหนึ่งในการรักษาความปลอดภัยด้านการรักษาความถูกต้องของข้อมูล (Data Integrity) และด้านการป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation) คือการตรวจสอบความถูกต้องครบถ้วนของเอกสารอิเล็กทรอนิกส์ด้วยการสร้างชุดตัวแทนข้อมูล (Message Digest) และการลงลายมือชื่อดิจิทัล

ลายมือชื่อดิจิทัล หรือ “Digital Signature” ไม่ใช่การสแกนลายเซ็นบนกระดาษเก็บไว้ในรูปของไฟล์ภาพแบบดิจิตอล หรือการดีไซน์ลายเซ็นด้วยเครื่องมือกราฟิกในการวาดภาพ แล้วเก็บไว้เป็นไฟล์ดิจิตอล โดยจะแนบหรือแปะรูปของลายเซ็นนั้นลงในเอกสารแล้วส่งไปยังผู้รับแทนการส่งกระดาษที่มีลายเซ็นจริง และไม่ใช่การนำปากกาสำหรับเขียนบนหน้าจอทัชสกรีนเขียนลายเซ็นลงบนหน้าจอต่างๆ แล้วนำภาพลายเซ็นนั้นไปใช้

ความสำคัญของลายเซ็นบนเอกสารที่เซ็นด้วยปากกาหรือเครื่องเขียนอื่น เป็นการลงนามเพื่อรับรองถึงการรับทราบและเห็นด้วยกับรายละเอียดเนื้อความที่ปรากฏในเอกสารนั้นๆ ดังนั้น “ลายเซ็น” หรือ “ลายมือชื่อ” จึงถือว่ามีความสำคัญเป็นอย่างยิ่งในการแสดงตัวตนและพิสูจน์ตัวตนประกอบการทำธุรกรรมต่างๆ ของบุคคลในหน่วยงาน ซึ่งในบางครั้งมักพบปัญหาการปฏิเสธว่าไม่รู้ไม่เห็นจากเจ้าของลายเซ็นในเอกสารเกิดขึ้น โดยกล่าวอ้างว่าถูกปลอมแปลงลายเซ็นโดยบุคคลอื่น หรือบางครั้งก็จะพบกับปัญหาการปฏิเสธว่าไม่รู้ไม่เห็นเอกสารหน้าใดหน้าหนึ่งหรือหลายหน้า โดยกล่าวอ้างว่ามีการเปลี่ยนแปลงบางส่วนของเอกสารหรือมีการตัดทอนหรือสอดแทรกเอกสารใหม่บางส่วนโดยผู้ไม่ประสงค์ดี

ลายมือชื่อดิจิทัลถูกคิดค้นขึ้นเพื่อที่จะนำมาใช้ประโยชน์ในการแสดงตัวตนและพิสูจน์ตัวตนของบุคคล (หรือหน่วยงาน) ในกรณีที่มีการรับทราบและเห็นด้วยกับรายละเอียดเนื้อความที่ปรากฏในเอกสารแบบอิเล็กทรอนิกส์นั้นๆ โดยอาศัยกระบวนการคำนวณทางคณิตศาสตร์ที่ประมวลผลโดยคอมพิวเตอร์แทนการใช้ปากกาลงลายมือชื่อบนกระดาษ ซึ่งหลักการและวิธีการของลายเซ็นอิเล็กทรอนิกส์นั้นถือเป็นนวัตกรรมในด้านการแสดงตัวตนและพิสูจน์ตัวตนเพื่อทำธุรกรรมบนโลกไซเบอร์ให้ได้อย่างปลอดภัยและมีประสิทธิภาพอย่างแท้จริง เทคโนโลยีนี้สามารถป้องกันการเกิดปัญหาการปฏิเสธว่าไม่รู้ไม่เห็น ไม่ได้เซ็นด้วยตัวเอง หรือปฏิเสธว่าไม่เคยรู้เคยเห็นบางส่วนของเนื้อความใน

เอกสาร แบบที่พบได้ในโลกของการทำธุรกรรมแบบลงลายมือชื่อด้วยปากกาหรือเครื่องเขียนอื่น โดยมีรายละเอียด ดังนี้

❒ ความหมายและความสำคัญ

สมมุติว่า “สมชาย” อ่านเอกสารสัญญาที่ทำกับ “สมหญิง” ที่ถูกส่งมาให้ทางอีเมลในรูปของไฟล์อิเล็กทรอนิกส์ และเห็นด้วยกับเนื้อหาที่ปรากฏในเอกสารสัญญานั้นทั้งหมด จึงตอบตกลงกับสมหญิงว่ายอมรับตามเงื่อนไขที่ระบุทั้งหมด ซึ่งการตอบตกลงของสมชายจะต้องเป็นการตอบตกลงที่พิสูจน์ยืนยันได้ว่า “สมชาย” เป็นผู้ตอบตกลงจริงด้วยตัวเอง ซึ่งจุดสำคัญที่สุดตรงนี้ก็คือ คำว่า “พิสูจน์ยืนยันได้” นั้นหมายความถึง ๒ สิ่งสำคัญ ได้แก่ (๑) เป็นการตอบตกลงกับเนื้อหาที่ระบุในสัญญานั้นทั้งหมด (ทุกส่วนตั้งแต่หน้าแรกจนถึงหน้าสุดท้าย) และ (๒) ไม่สามารถปฏิเสธในภายหลังได้ว่าตัวเองไม่ได้เป็นผู้เซ็นยอมรับ (ถูกผู้อื่นแอบอ้างว่าเป็นตัวเอง) ซึ่งระบบลายมือชื่อดิจิทัลจะต้องสามารถให้ความเชื่อถือและพิสูจน์ยืนยันได้ถึง ๒ สิ่งสำคัญดังกล่าว แม้กระทั่งใช้เป็นตัวพิสูจน์ความถูกต้องในชั้นศาล

❒ หลักการของลายมือชื่อดิจิทัล

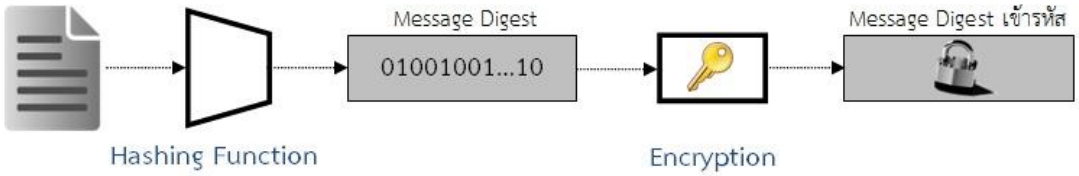
กระบวนการพิสูจน์ยืนยันจะใช้หลักการคำนวณทางคณิตศาสตร์ชั้นสูง โดยการใช้ประโยชน์จากกระบวนการเข้ารหัสข้อมูลแบบอสมมาตร (Asymmetric Key Encryption) ซึ่งวิธีการเข้ารหัสข้อมูลชนิดนี้จะใช้กุญแจในการเข้ารหัสและกุญแจในการถอดรหัสที่แตกต่างกัน โดยกุญแจที่ใช้ในการเข้ารหัสจะเรียกว่า “กุญแจส่วนตัว (Private Key)” และกุญแจที่ใช้ในการถอดรหัสจะเรียกว่า “กุญแจสาธารณะ (Public Key)” โดยกุญแจทั้ง ๒ ชนิดนี้ จะมีอยู่เป็นชุดคู่กันเสมอ และกุญแจส่วนตัว (Private Key) นั้นจะรู้เฉพาะเจ้าของซึ่งก็คือสมชายเท่านั้น ส่วนกุญแจสาธารณะ (Public Key) นั้น จะประกาศสู่สาธารณะเพื่อให้ทุกคนที่จะติดต่อกับสมชายรับทราบ และสมหญิงก็เป็นหนึ่งในผู้ที่รับทราบถึงกุญแจสาธารณะของสมชายดังกล่าว

หลักการที่สำคัญคือ ไฟล์เอกสารสัญญาที่ถูกเข้ารหัสโดยกุญแจส่วนตัวของสมชายจะสามารถทำการถอดรหัสได้ด้วยกุญแจสาธารณะที่เป็นชุดคู่กัน โดยไม่จำเป็นที่จะต้องทราบถึงกุญแจที่ใช้ในการเข้ารหัส (กุญแจส่วนตัวของสมชาย) แต่อย่างใด ซึ่งแตกต่างจากกระบวนการเข้ารหัสแบบสมมาตร (Symmetric Key Encryption) ซึ่งเป็นวิธีการเข้ารหัสข้อมูลทั่วไปที่ใช้กุญแจในการเข้ารหัสและถอดรหัสตัวเดียวกัน โดยเรียกกุญแจที่ใช้ในการเข้ารหัสและถอดรหัสว่า “กุญแจลับ” หรือ “Secret Key” และผู้ส่ง (ผู้ที่เข้ารหัส) กับผู้รับ (ผู้ที่ถอดรหัส) จะต้องทราบและใช้กุญแจค่าเดียวกันเสมอ (ภาพที่ ๒.๕)

ตรงนี้ มีนัยสำคัญอย่างยิ่ง ๒ อย่างคือ (๑) สมหญิง (และผู้อื่นที่ติดต่อกับสมชาย) จะไม่ทราบถึงค่าของกุญแจที่ใช้ในการเข้ารหัสของสมชายเลย ในขณะที่สามารถถอดรหัสไฟล์เอกสารสัญญาได้อย่างถูกต้อง และ (๒) หากกุญแจสาธารณะของสมหญิง (และผู้อื่นที่ติดต่อกับสมชาย) สามารถใช้ทำการถอดรหัสข้อมูลที่ถูกเข้ารหัสด้วยกุญแจส่วนตัวของสมชายได้ แสดงว่าข้อมูลนั้นถูกเข้ารหัสโดยกุญแจส่วนตัวของสมชายซึ่งมีสมชายเท่านั้นที่รู้ค่าของกุญแจนี้ โดย ๒ ข้อของนัยสำคัญนี้เองที่เป็นตัวพิสูจน์ยืนยันได้ถึงการป้องกันการปฏิเสธว่าไม่ได้เซ็นด้วยตัวเองของผู้ส่งได้ เนื่องจากไม่มีคนอื่นใดที่จะรู้ค่าของกุญแจส่วนตัวที่ใช้ในการเข้ารหัสนอกจากผู้ส่งหรือสมชายเพียงคนเดียวเท่านั้น

ภาพที่ ๒.๕ หลักการของลายมือชื่อดิจิทัล

การป้องกันการปฏิเสธว่าไม่เคยรู้เคยเห็นบางส่วนของเนื้อความในเอกสาร (การกล่าวอ้างว่าบางส่วนของเอกสารถูกแก้ไขเปลี่ยนแปลง ตัดออก หรือเพิ่มเติมเข้าไป) นั้น จะใช้กระบวนการย่อข้อมูลหรือหาค่าของตัวแทนของข้อมูลที่เรียกว่า “Message Digest” โดยใช้วิธีนำข้อมูลขนาดใดๆ มาใส่เป็นค่า Input ของฟังก์ชั่นย่อข้อมูลทางคณิตศาสตร์แบบทางเดียวที่เรียกว่า One-way Hash Function ซึ่งจะให้ค่าของ Output ที่มีขนาดความยาวคงที่ เช่น ๑๒๘ บิต (ภาพที่ ๒.๖) โดยฟังก์ชั่นทางคณิตศาสตร์ดังกล่าว มีคุณสมบัติที่สำคัญคือ (๑) ถ้าข้อมูลต้นฉบับต่างกัน Message Digest ของทั้งสองจะต้องต่างกัน และ (๒) การคำนวณย้อนหาข้อมูลต้นฉบับจาก Message Digest กระทำได้ยากมากหรือไม่ได้เลยในเชิงการคำนวณแบบคณิตศาสตร์ด้วยคอมพิวเตอร์ภายใต้ทรัพยากรและเวลาที่มี

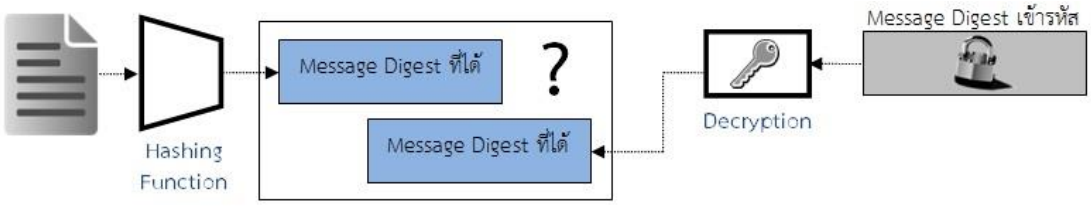


ภาพที่ ๒.๖ การสร้างชุดตัวแทนข้อมูล (Message Digest)

จากการนำกระบวนการย่อข้อมูลดังกล่าวข้างต้นมาใช้ ทำให้สมชายสามารถย่อขนาดของไฟล์เอกสารสัญญาที่อาจจะมีจำนวนหลายร้อยหน้าหรือหลายพันหน้า (มีขนาดหลาย MB) ลงมาเป็นค่าตัวแทนของข้อมูล หรือ “Message Digest” ที่มีความยาวข้อมูลเพียง ๑๒๘ บิต (ความยาว ๑๖ ตัวอักษร) ได้ โดยหลังจากนั้นสมชายจะใช้วิธีการนำข้อมูล Message Digest ดังกล่าวมาเข้ารหัสด้วยกุญแจส่วนตัวของสมชายเอง (กลไกการเข้ารหัสสามารถทำได้อย่างรวดเร็วเนื่องจากเป็นการเข้ารหัสข้อมูลที่มีขนาดเล็กมากเพียง ๑๒๘ บิต) แล้วแนบค่า Message Digest ที่ถูกเข้ารหัสไปพร้อมกับไฟล์เอกสารสัญญาที่มีข้อความครบถ้วนเพื่อส่งกลับไปให้สมหญิง สิ่งที่เกิดขึ้นก็คือ สมหญิงได้รับ (๑) ไฟล์

เอกสารสัญญาที่มีรายละเอียดทั้งหมดที่สมชายเห็นชอบด้วยและตกลงทำสัญญา (๒) ค่า Message Digest ของไฟล์เอกสารที่ถูกเข้ารหัสด้วยกุญแจส่วนตัวของสมชาย

หลังจากที่สมหญิงได้รับข้อมูลทั้ง ๒ ส่วนจากสมชายก็คือ (๑) สมหญิงนำไฟล์เอกสารสัญญามาผ่านกระบวนการย่อข้อมูลเพื่อหา Message Digest แบบเดียวกับที่สมชายทำ (กลไกการย่อข้อมูลเป็นกลไกที่เปิดเผยโดยทั่วไป เมื่อใช้กลไกแบบเดียวกันกับค่าของ Input Data เดียวกัน จะได้ค่าของ Output Data เดียวกันเสมอ) (๒) สมหญิงนำค่าของ Message Digest เข้ารหัสมาทำการถอดรหัสด้วยกุญแจสาธารณะ (Public Key) ของสมชายเพื่อหาค่า Message Digest เดิมก่อนถูกเข้ารหัสด้วยกุญแจส่วนตัวของสมชาย และ (๓) เปรียบเทียบค่าของ Message Digest ที่ได้จากข้อ ๒ และ ๓ โดยหากมีค่าเท่ากันแสดงว่าเอกสารสัญญานั้นเป็นเอกสารสัญญาที่สมชายยอมรับในเนื้อความทั้งหมดทุกส่วนด้วยตัวเองอย่างครบถ้วน (ภาพที่ ๒.๗)



ภาพที่ ๒.๗ การตรวจพิสูจน์ความถูกต้องครบถ้วนของเอกสาร

ทั้งนี้ จุดสำคัญก็คือ หากมีการเปลี่ยนเนื้อความส่วนใดส่วนหนึ่งของไฟล์เอกสาร ไม่ว่าจะด้วยการเพิ่ม ลด สอดแทรก ฯลฯ จะส่งผลทำให้ค่าของ Message Digest ที่ได้จากข้อ ๑ มีค่าเปลี่ยนแปลงไป โดยค่าที่ได้จะไม่ตรงกันกับค่าของ Message Digest ในข้อ ๒ ที่ได้จากการถอดรหัสด้วยกุญแจสาธารณะของสมชาย (ซึ่งเป็นค่า Message Digest ของไฟล์เอกสารสัญญาที่ไม่มีการเปลี่ยนแปลงแก้ไขใดๆ) ทั้งนี้และทั้งนั้น ความพยายามในการเปลี่ยนแปลงแก้ไขส่วนใดส่วนหนึ่งของเนื้อหาในไฟล์เอกสารโดยคงไว้ซึ่งค่าของ Message Digest เดิม (คือค่าที่ได้จากการถอดรหัสในข้อ ๒) จะกระทำได้ยากมากหรือกระทำไม่ได้เลยในการคำนวณเชิงคณิตศาสตร์ด้วยคอมพิวเตอร์ ดังนั้น หากค่าที่ได้ “เท่ากัน” ก็จะเป็นการพิสูจน์ยืนยันว่าสมชายเป็นผู้ส่งข้อมูลนั้นมาด้วยตัวเอง และเนื้อความในสัญญาทั้งหมดทุกส่วนตามที่ระบุในเอกสารสัญญาที่แนบมาตรงกันกับที่สมชายอ่าน

❒ หน่วยงานกลางที่เกี่ยวข้อง

สิ่งสำคัญอย่างยิ่งคือ จะเชื่อได้อย่างไรว่ากุญแจสาธารณะที่สมหญิงมีอยู่นั้นเป็นกุญแจสาธารณะของสมชายจริง กล่าวคือ อาจจะมีผู้ไม่ประสงค์ดีแอบอ้างตัวเป็นสมชายแล้วบอกค่ากุญแจสาธารณะของตัวเองให้กับสมหญิงก็เป็นได้ เพื่อที่จะยืนยันถึงความมีตัวตนและเป็นเจ้าของกุญแจส่วนตัวที่เป็นชุดคู่กับกุญแจสาธารณะนั้นจริง จำเป็นที่จะต้องมีหน่วยงานกลางที่มีความน่าเชื่อถือทำการลงทะเบียนข้อมูลของสมชายเอาไว้ แล้วเผยแพร่ค่ากุญแจสาธารณะของสมชายให้ผู้ที่เกี่ยวข้องทราบ เสมือนกับว่ามีที่ทำการอำเภอที่สามารถยืนยันความมีตัวตนและเป็นตัวตนที่แท้จริงของสมชายได้ การยืนยันถึงการมีตัวตนที่แท้จริงของสมชายสามารถทำได้โดยการจัดตั้งองค์กรกลางที่ให้การ

รับรองที่เรียกว่า Certificate Authority (CA) โดยองค์กรนี้จะทำการออกใบรับรองว่ากุญแจสาธารณะนั้นเป็นของสมชายจริงตามที่ได้กล่าวอ้างไว้ ซึ่งใบรับรองนั้นจะเป็นใบรับรองแบบอิเล็กทรอนิกส์ที่เรียกว่า Digital Certificate ที่ออกตามมาตรฐาน X.509 (มาตรฐานที่ได้รับความเชื่อถือและใช้งานในปัจจุบัน) ทั้งนี้ก็เพื่อเป็นการป้องกันการแอบอ้างว่าเป็นเจ้าของกุญแจสาธารณะจากผู้ไม่ประสงค์ดีนั่นเอง

๒.๓ เทคโนโลยี BLOCKCHAIN

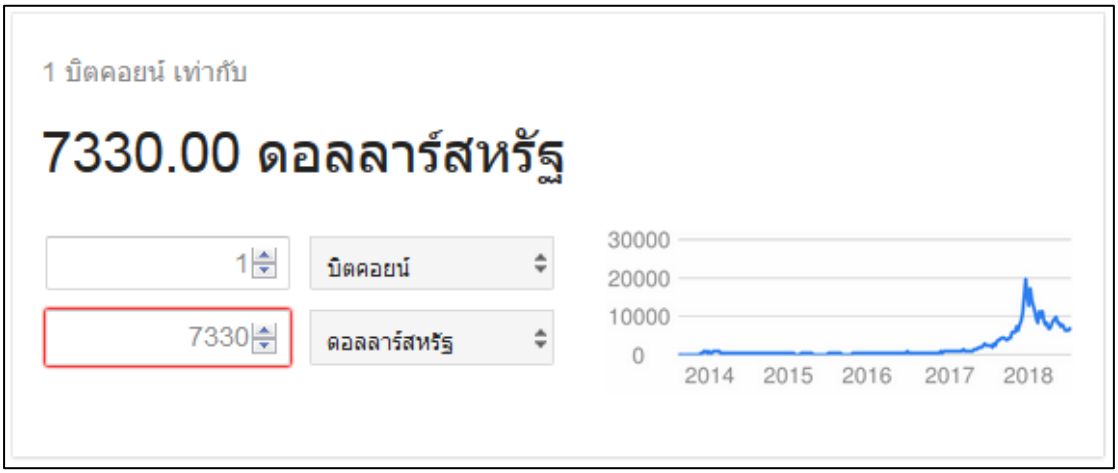
เทคโนโลยีที่กำลังถูกจับตามองว่ากำลังมาแรงและเป็นเทคโนโลยีที่สามารถปฏิวัติระบบการทำธุรกรรมแบบออนไลน์ในลักษณะที่เปลี่ยนรูปแบบไปจากเดิมอย่างสิ้นเชิง ได้แก่ เทคโนโลยีที่เรียกว่า “BLOCKCHAIN”

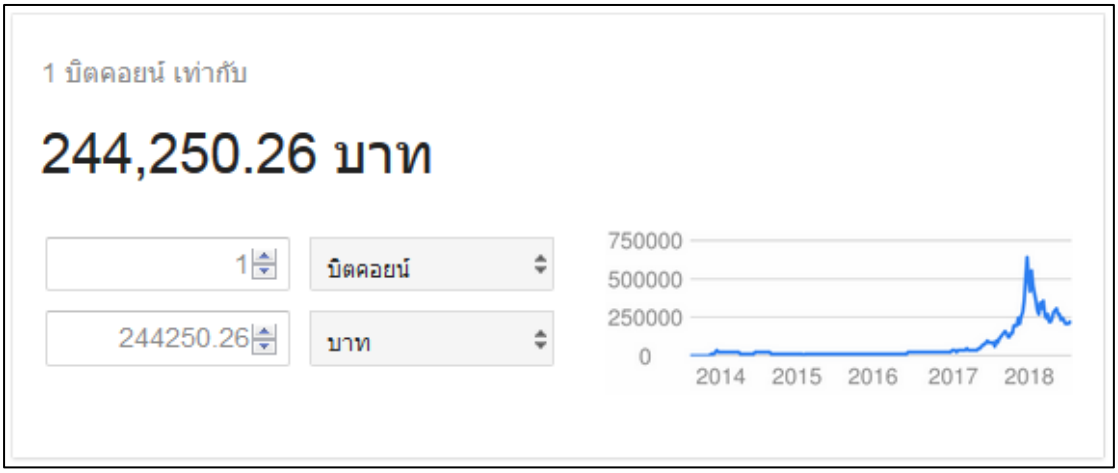
ปัจจุบันรูปแบบของการทำธุรกรรมแบบออนไลน์ในโลกอินเทอร์เน็ต โดยเฉพาะธุรกรรมเกี่ยวกับการเงิน จำเป็นต้องมีองค์กรหรือหน่วยงานกลางที่ทำหน้าที่เป็นศูนย์กลางของการทำธุรกรรมทั้งมวล เนื่องจากผู้ทำธุรกรรมต้องการหน่วยงานกลางที่สามารถ “เชื่อถือและไว้วางใจได้” มาทำหน้าที่เสมือนเป็นสะพานเชื่อมระหว่างผู้ทำธุรกรรมและผู้ร่วมทำธุรกรรมนั้นๆ ตัวอย่างที่เข้าใจได้ง่ายที่สุด ได้แก่ การทำธุรกรรมการเงินผ่าน “ธนาคาร” เช่น หากนาย ก. โอนเงินให้นาย ข. เป็นจำนวน ๕,๐๐๐ บาท โดยไม่ผ่านหน่วยงานกลางใดๆ ภายหลังจากที่ได้รับเงินแล้ว นาย ข.อาจปฏิเสธได้ว่ายังไม่ได้รับเงิน หรืออาจกล่าวอ้างได้ว่าได้รับเงินโอนมาแล้วเพียงจำนวน ๑,๐๐๐ บาทเท่านั้น เพราะหลักฐานที่จะใช้พิสูจน์ความถูกต้องก็จะมีถือครองเฉพาะ นาย ก.และ นาย ข. เท่านั้น โดยในกรณีนี้นาย ข.สามารถทำลายหลักฐานทิ้งไป พร้อมกล่าวอ้างว่าหลักฐานที่นาย ก. มีนั้นเป็นหลักฐานเท็จที่สร้างขึ้นมาเอง

ตรงนี้คงจะเห็นภาพได้ชัดเจนขึ้นถึงความสำคัญและจำเป็นในการที่จะต้องมีหน่วยงานกลางที่เชื่อถือและไว้วางใจได้ เช่น “ธนาคาร” เข้ามาเป็นตัวกลางในการทำธุรกรรม เนื่องจาก ธนาคารจะเป็นผู้ดำเนินการและจัดเก็บหลักฐานในการทำธุรกรรมที่เกิดขึ้นทั้งหมดไว้อย่างปลอดภัย โดยทั้ง นาย ก. และ นาย ข. จะได้รับมอบเพียงสมุดบัญชีธนาคารที่มีระบุหมายเลขบัญชีธนาคาร (Account Number) และยอดเงินปัจจุบันกับรายการพิมพ์ประวัติการทำธุรกรรม (ฝาก, ถอน, โอน ฯลฯ) จากระบบคอมพิวเตอร์ของธนาคารที่บันทึกอยู่ภายใน ไม่สามารถแอบอ้างหรือเปลี่ยนแปลงแก้ไขใดๆได้เอง ทำให้ผู้ทำธุรกรรมและผู้ร่วมทำธุรกรรมซึ่งอาจเป็นผู้ใดก็ได้ โดยเฉพาะธุรกรรมแบบออนไลน์ในโลกอินเทอร์เน็ต เชื่อใจและมั่นใจในการทำธุรกรรมต่างๆ

ปัจจุบัน เทคโนโลยีที่เรียกว่า “BLOCKCHAIN” กำลังจะเข้ามาปฏิวัติรูปแบบการทำธุรกรรมแบบดั้งเดิมที่ต้องมีหน่วยงานกลางที่เชื่อถือและไว้ใจได้ดังกล่าว ให้เป็นลักษณะที่ผู้ทำธุรกรรมและผู้ร่วมทำธุรกรรมใดๆสามารถดำเนินการโดยตรงได้เองโดยไม่ผ่านหน่วยงานกลาง และที่สำคัญคือสามารถการันตีในความเชื่อถือและไว้ใจได้ของระบบธุรกรรมแบบ BLOCKCHAIN ว่ามีความถูกต้องปลอดภัย โดยจะไม่มีผู้ใดสามารถบอกปฏิเสธหรือกล่าวอ้างให้เป็นอย่างอื่นนอกเหนือจากธุรกรรมที่เกิดขึ้นจริงได้ และไม่มี Hacker ใดๆ สามารถเข้าไปทำลายหรือแก้ไขเปลี่ยนแปลงข้อมูลได้ภายใต้เทคโนโลยีการประมวลผลในปัจจุบันอีกด้วย

แนวคิดของ BLOCKCHAIN เกิดขึ้นมาพร้อมๆกับแนวคิดเรื่องสกุลเงินดิจิทัล (Digital Money) หรือเงินในรูปแบบของดิจิทัลที่จัดเก็บอยู่ในกระเป๋าเงินดิจิทัลที่เรียกว่า “**Digital Wallet**” สามารถนำมาจับจ่ายใช้สอย (ฝาก, โอน, จ่ายหรือชำระ ฯลฯ) ในการทำธุรกรรมต่างๆ ได้จริง สกุลเงินที่เป็นที่รู้จักกันมากที่สุดก็คือสกุลเงินที่เรียกว่า “**Bitcoin**” ที่จัดเก็บอยู่ในกระเป๋าเงินดิจิทัลที่เรียกว่า “**Bitcoin Wallet**” ซึ่งมีผู้เข้าร่วมใช้งานอยู่เป็นจำนวนมาก จริงๆแล้ว แม้ว่าในปัจจุบัน Bitcoin ยังไม่ถือว่าเป็นเงินที่สามารถชำระหนี้ได้ตามกฎหมายและปราศจากการควบคุมของธนาคารกลางหรือภาครัฐ แต่ก็ถูกใช้ในแวดวงของผู้ที่เข้าร่วมใช้งานทั่วโลกโดยมีการกำหนดมูลค่าในการแลกเปลี่ยนขึ้น โดยปัจจุบันพบว่าอัตราแลกเปลี่ยนทั่วไปอยู่ที่ประมาณ 7,330 US$ (244,250 บาท) ต่อ 1 Bitcoin (ภาพที่ ๒.๘)



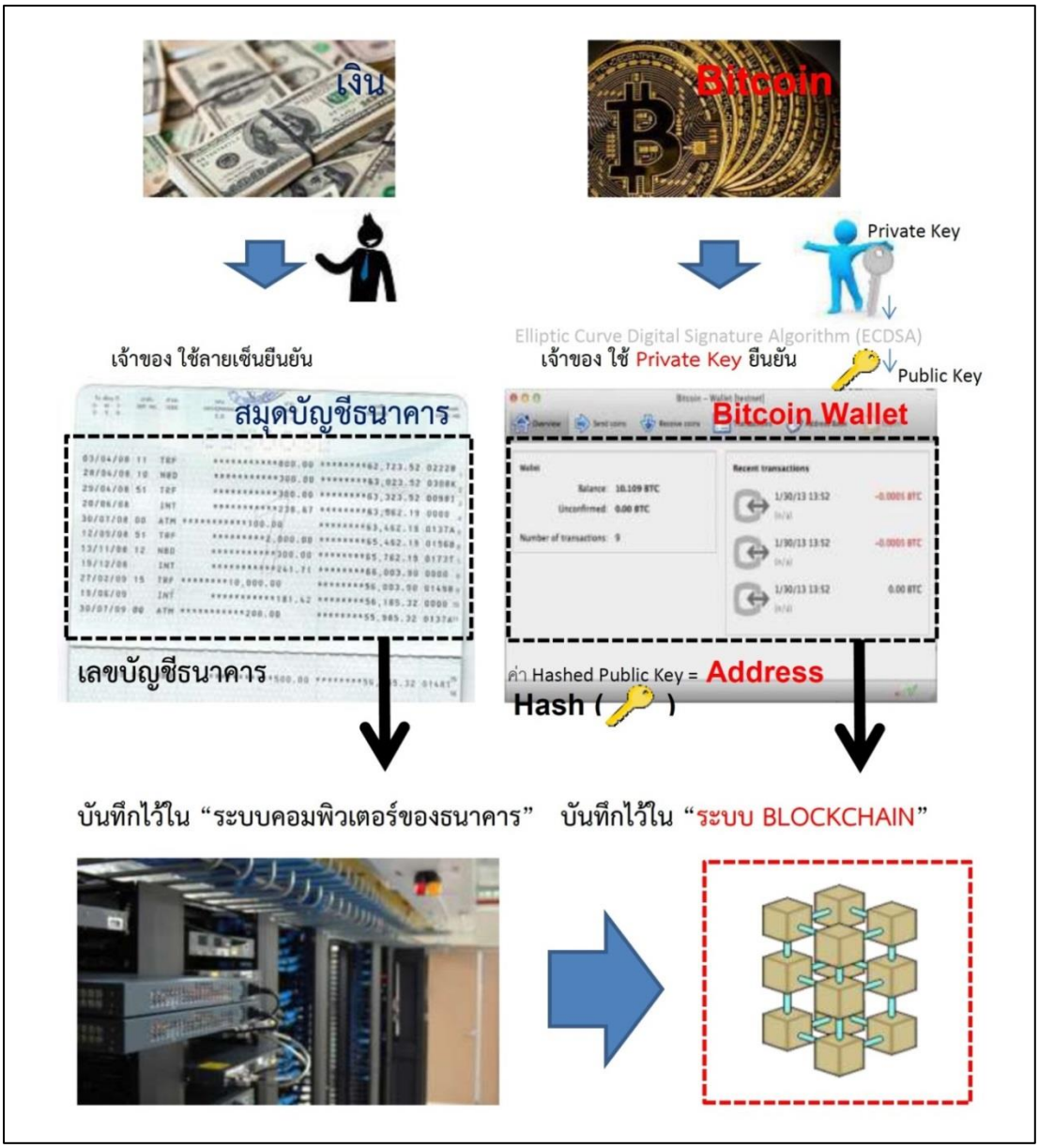


* ที่มา www.coindesk.com/price/ (อัตราแลกเปลี่ยน ณ วันที่ ๒๑ ก.ค.๖๑)

ภาพที่ ๒.๘ อัตราแลกเปลี่ยน Bitcoin

เพื่อให้เกิดภาพที่ช่วยทำให้เข้าใจในกลไกต่างๆของ BLOCKCHAIN กับระบบการทำงานร่วมกับ Bitcoin ซึ่งเป็นรูปแบบการใช้งานกับระบบการเงิน ขอยกตัวอย่างของระบบธนาคารในปัจจุบันที่ใช้

ระบบสกุลเงินสากลและมีการออกสมุดบัญชีที่มีระบุหมายเลขบัญชี (Bank Account) ของผู้เป็นเจ้าของ โดยใช้ลายมือชื่อหรือลายเซ็นเป็นสิ่งยืนยันตัวตนที่แท้จริงของผู้เป็นเจ้าของ และมีการบันทึกการทำธุรกรรม (Transactions) ของบัญชีธนาคารนั้นๆ ไว้ในระบบคอมพิวเตอร์ของธนาคาร โดยสามารถจัดพิมพ์รายการธุรกรรมต่างๆลงในสมุดบัญชีเพื่อเรียกดูได้ตามต้องการ เปรียบเทียบกับตัวอย่างรูปแบบของการทำงานของ BLOCKCHAIN ที่ใช้สกุลเงิน Bitcoin โดยมีการออกแบบระบบให้ทำงานภายใต้เทคโนโลยีการเข้ารหัสแบบกุญแจสาธารณะ (Public Key Cryptography) หรือการเข้ารหัสแบบกุญแจอสมมาตร (Asymmetric Key Encryption) ที่ใช้ประโยชน์จากกุญแจส่วนตัว (Private Key) ซึ่งมีผู้เป็นเจ้าของที่แท้จริงเท่านั้นที่ทราบค่าของกุญแจ ร่วมกับกุญแจสาธารณะ (Public Key) ที่เป็นคู่กับกุญแจส่วนตัวนั้นๆ โดยกุญแจสาธารณะดังกล่าวจะทำงานร่วมกับกุญแจส่วนบุคคลที่เป็นคู่กันได้เท่านั้น (ภาพที่ ๒.๙)



ภาพที่ ๒.๙ กลไกการทำงานของ BLOCKCHAIN กับสกุลเงิน Bitcoin

ในที่นี้ Bitcoin จะแทนเงินในสกุลสากลแบบปกติที่ใช้งานในปัจจุบัน โดยมี Bitcoin Wallet แทนสมุดบัญชีธนาคาร ซึ่งในระบบธนาคารปกตินั้น จะใช้ลายมือชื่อหรือลายเซ็นของเจ้าของบัญชีในการตรวจสอบและยืนยันความเป็นเจ้าของที่แท้จริง แต่ในระบบการเงิน Bitcoin นั้น จะใช้ค่าของกุญแจส่วนตัว (Private Key) ซึ่งทราบเฉพาะเจ้าของเพียงคนเดียวเท่านั้น เป็นสิ่งตรวจสอบและยืนยันความเป็นเจ้าของที่แท้จริงของ Bitcoin Wallet นั้น นอกจากนี้ ยังมีค่าที่เรียกว่า “**Address**” ซึ่งใช้แทนหมายเลขบัญชีธนาคาร โดยค่าของ Address ดังกล่าวเป็นค่าที่คำนวณมาจากการทำ Hashing กับกุญแจสาธารณะ (Public Key) ที่เข้าคู่กันกับกุญแจส่วนตัวนั้น ซึ่งการทำ Hashing นั้นจะใช้ฟังก์ชั่นพิเศษชั้นสูงทางคณิตศาสตร์ในลักษณะของฟังก์ชั่นทางเดียว (One-way Function) ในการคำนวณ บนพื้นฐานที่ว่า ค่า Input ใดๆที่แตกต่างกัน จะให้ค่า Output ที่แตกต่างกัน และการคำนวณหาค่าของ Input ย้อนกลับจากค่า Output เป็นสิ่งที่ปฏิบัติไม่ได้ ทำได้เพียงการ Brute Force ลองทุกค่า Input ที่เป็นไปได้

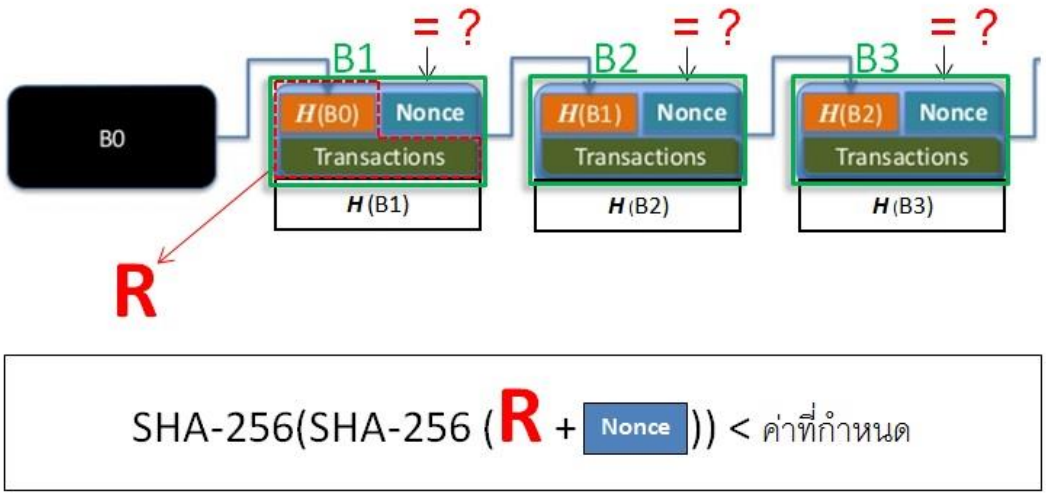
ตรงนี้ สิ่งที่เป็นส่วนสำคัญก็คือ ระบบธนาคารปกติในปัจจุบัน จะใช้วิธีการบันทึกธุรกรรม (Transactions) ทั้งหมดไว้ในระบบคอมพิวเตอร์ของธนาคาร ซึ่งถือเป็นวิธีการจัดเก็บและประมวลผลแบบรวมศูนย์ (Centralized System) โดยมีธนาคารเป็นหน่วยงานกลางที่ผู้ทำธุรกรรมและผู้ร่วมทำธุรกรรมเชื่อถือและไว้วางใจ ทำให้เกิดค่าใช้จ่ายในลักษณะของค่าธรรมเนียมต่างๆขึ้น โดยเฉพาะเมื่อต้องทำธุรกรรมข้ามประเทศหรือข้ามสกุลเงิน นอกจากนี้ ในหลายกรณี ยังต้องประสบกับปัญหาการแสดงเอกสารหรือหลักฐานต่างๆประกอบทำให้เกิดความยุ่งยากตามมาอีกด้วย

เทคโนโลยี BLOCKCHAIN คือระบบการจัดการฐานข้อมูลรูปแบบใหม่ ถือกำเนิดขึ้นมาเพื่อที่จะตัดวงจรของหน่วยงานกลางดังกล่าวออกไปจากวงรอบการทำธุรกรรมใดๆ ด้วยการกำหนดกลไกการบันทึกการทำธุรกรรมทั้งหมดเอาไว้ในลักษณะของห่วงโซ่ (Chain) ของกลุ่มข้อมูล (Block) และจัดเก็บข้อมูลไว้กับผู้ร่วมทำธุรกรรม (ซึ่งเรียกว่า Node) ทั้งหมด เพื่อการจัดทำ “บัญชีธุรกรรม (Ledger)” แบบกระจายตัว (Distributed) สำหรับบันทึกเส้นทางการทำธุรกรรมและตรวจสอบความถูกต้อง โดยเมื่อใดก็ตามที่มีธุรกรรม (Transaction) เกิดขึ้น ข้อมูลจะถูกอัพเดทไปยังห่วงโซ่ข้อมูลของทุกคนทันทีแบบ Real-time ทั้งนี้ ประเด็นที่สำคัญที่สุดคือ ระบบ BLOCKCHAIN นั้น การันตีถึงความถูกต้องและเชื่อถือได้ของการทำธุรกรรมของผู้ใช้บริการทุกคนในระบบแม้จะไม่มีหน่วยงานกลางก็ตาม ซึ่งขยายความรวมถึงการไม่สามารถ ปฏิเสธ/แก้ไข/เปลี่ยนแปลง/บิดเบือน ข้อมูลใดๆที่เกี่ยวข้องกับการทำธุรกรรมได้อีกด้วย

โครงสร้างของ BLOCKCHAIN นั้น แบ่งกลุ่มของข้อมูลธุรกรรมออกเป็นลักษณะของ Block แล้วนำ Block ของธุรกรรมที่เกิดขึ้นตามมาต่อพ่วงเพิ่มเติมเข้าไปตามลำดับ โดย Block ถัดไปจะมีค่า Hash ของ Block ก่อนหน้าไว้ตรวจสอบความถูกต้องของข้อมูลใน BLOCKCHAIN เสมอ ทำให้การแก้ไขข้อมูลใดๆใน Block ใดๆ ไม่สามารถกระทำได้ เพราะจะทำให้ BLOCKCHAIN เกิดค่าผิดพลาดทั้งระบบ ส่วนประกอบหลักๆในแต่ละ Block ประกอบด้วย

๑. ส่วน Header ของแต่ละ Block
   (* รวมค่า Hash ของ Block ก่อนหน้า และ Nonce ซึ่งเป็นค่าพิเศษใดๆ)
๒. ส่วนธุรกรรม (Transactions)
๓. ค่า Hash ของ Block นั้นๆ

โดยผู้ที่ทำธุรกรรมจะเป็นผู้ประกาศ Transaction(s) นั้นออกไปในเครือข่ายผู้ใช้งานทั้งหมด ซึ่งในกลไกของ BLOCKCHAIN จะมีผู้ร่วมพิเศษในระบบที่ทำหน้าที่ตรวจสอบยืนยันความถูกต้องของ Transaction(s) ที่เรียกว่า “**Miner**” ซึ่งมีระบบคอมพิวเตอร์และการประมวลผลที่มากพอ เพื่อตรวจสอบว่า Transaction(s) ดังกล่าวนั้นถูกต้องหรือไม่ (ใครทำธุรกรรมกับใคร เงินเพียงพอหรือไม่ ฯลฯ) แต่ต้องแก้โจทย์พิเศษที่ผู้สร้างระบบ BLOCKCHAIN กำหนดขึ้นด้วย ได้แก่การหาค่า “**Nonce**” ที่ทำให้สมการค่า Hash (ใช้ Double SHA-256) ได้ผลลัพธ์น้อยกว่าค่าที่กำหนด (ภาพที่ ๒.๑๐) ซึ่งในการแก้ปัญหาโจทย์พิเศษนั้นจำเป็นต้องใช้ทรัพยากรทางการประมวลผลสูงเพื่อคำนวณหาค่าที่เป็นคำตอบ โดยเมื่อ Miner ตรวจสอบความถูกต้องของ Transactions และแก้ปัญหาโจทย์ได้แล้ว จะใส่ค่า Nonce ลงใน Block และคำนวณค่า Hash ของทั้ง Block แล้วผนึกข้อมูลทั้งหมดลงเป็น Block สมบูรณ์แล้วนำกระจายส่งไปต่อพ่วงให้กับข้อมูล BLOCKCHAIN ของทุกคนในระบบ (ทุกคนจะมีชุดข้อมูลเดียวกัน อัพเดทเหมือนกัน)



ภาพที่ ๒.๑๐ การแก้โจทย์ปัญหาของ Miner

ในการแก้โจทย์ปัญหาพิเศษนั้น จะใช้วิธีแข่งขันระหว่างผู้ที่เป็น Miner ทั้งหลาย โดยใครคำนวณค่าได้สำเร็จก่อน ก็จะได้รับรางวัลเป็น Bitcoin จำนวนหนึ่งตอบแทน (และอาจได้ค่า Transaction Fee เป็น Bitcoin จากผู้ทำธุรกรรมด้วย) ซึ่งในการตรวจยืนยันความถูกต้องของ Transaction(s) ใดๆ ที่ถูกส่งออกมาเพื่อขอการรับรองและการตอบโจทย์ปัญหาพิเศษ จะมี Miner เพียงเจ้าเดียวเท่านั้นที่จะได้รับรางวัลตอบแทน ซึ่งก็คือผู้ที่ทำได้สำเร็จก่อน

เทคโนโลยี BLOCKCHAIN สามารถประยุกต์ใช้กับการทำธุรกรรมประเภทอื่นนอกเหนือจากการเงิน แบบที่ไม่ต้องมีหน่วยงานกลางแต่สามารถการันตี “ความถูกต้องและความเชื่อถือ” ให้กับผู้ใช้งานทุกคนในทุกธุรกรรมได้ โดยในการประยุกต์ใช้นั้น ต้องมีการออกแบบ Transaction/การตรวจสอบ ให้มีความเหมาะสมกับลักษณะของงานด้วย

บทที่ ๓
การกำหนดนโยบายด้านความปลอดภัย

หลายหน่วยงานยังไม่มีมาตรการในการที่จะป้องกันภัยคุกคามอย่างเป็นรูปธรรม โดยเฉพาะหน่วยงานที่ขาดบุคลากรด้าน IT ที่มีความเชี่ยวชาญเรื่องการรักษาความปลอดภัย และหน่วยงานราชการที่มีขนาดใหญ่ ประกอบไปด้วยบุคลากรที่หลากหลาย ทำให้การดูแล กำกับ และควบคุม ด้านการป้องกันภัยคุกคามทางไซเบอร์ ไม่สามารถกระทำได้อย่างมีประสิทธิภาพและประสิทธิผล ทำให้เกิดมีช่องโหว่ที่เปราะบางที่สุด (Weakest Link) เป็นจำนวนมาก ทั้งที่ระบบเครือข่ายคอมพิวเตอร์โดยรวมมีการป้องกันอย่างแน่นหนา ทั้งด้วยอุปกรณ์ป้องกันแบบ Hardware และ Software ก็ตาม

ปัญหาและความเสียหายอันอาจเกิดขึ้นได้ง่ายอย่างคาดไม่ถึงจาก Weakest Link ดังกล่าวในปัจจุบัน พบว่าเป็นเรื่องสำคัญที่สุดเรื่องหนึ่งที่หน่วยงานต้องตระหนักอย่างจริงจัง ซึ่งวิธีการในการป้องกันนั้น มีด้วยกันมากมายหลายวิธี ตั้งแต่ การหมั่นอัพเดทตัวระบบปฏิบัติการ (Patch Operating System), การบังคับใช้การกำหนดรหัสผ่านในระดับที่มีความปลอดภัย (Enforce a Strong Password Policy), การบล็อคเว็บไซต์อันตราย (Web Blocking), การเก็บข้อมูลการใช้งานระบบเครือข่าย (Network Activity Logging), การติดตั้ง Firewall, การเข้ารหัส TLS ระหว่าง Email Server, การใช้โปรแกรมป้องกันไวรัสและมัลแวร์, การจัดแบ่งส่วนของเครือข่าย (Network Segmentation), การกลั่นกรองเนื้อหาในเว็บ (Web Content Filtering), การตั้งค่าต่างๆ (Configurations), การทำ Blacklist ของ IP/Gateway, การเพิ่มองค์ประกอบในการพิสูจน์ตัวตน (Multi-factor Authentication), การให้ความรู้ด้านความปลอดภัยแก่ผู้ปฏิบัติ (User Education) และ วิธีการ/มาตรการ อื่นๆอีกเป็นจำนวนมาก ซึ่งการที่มีหลากหลาย วิธีการ/มาตรการ นี้เองที่ทำให้ยากต่อการปฏิบัติ และที่สำคัญ ไม่มีการวิเคราะห์และจัดลำดับความสำคัญของ วิธีการ/มาตรการ ที่จะส่งผลดีเชิงรูปธรรมได้มากที่สุด

การจัดการด้านความปลอดภัยของหน่วยงานนั้น มีความจำเป็นที่จะต้องกำหนดกลยุทธ์ด้านความปลอดภัยทางไซเบอร์เพื่อให้การจัดการหน่วยงานเป็นไปด้วยความปลอดภัยในแนวทางที่ชัดเจน หนึ่งในชุดของกลยุทธ์ที่ใช้ในการป้องกันภัยคุกคามทางไซเบอร์ที่น่าสนใจและสามารถนำมาใช้เป็นกรณีศึกษาในการหามาตรการป้องกันได้เป็นอย่างดี ได้แก่ กลยุทธ์ในการป้องกันที่เรียกว่า “**Catch-Patch-Match**” ของ Australian Signal Directorate, Department of Defence ที่มีการประกาศเพื่อเป็นแนวทางกลยุทธ์ในการป้องกันภัยคุกคามทางไซเบอร์ให้กับทั้งองค์กรภาครัฐและเอกชน โดยระบุไว้ว่า สามารถที่จะลดความเสี่ยงจากการถูกการโจมตีทางไซเบอร์ได้อย่างน้อยถึง ๘๕ % และที่สำคัญคือ ทำความเข้าใจได้ง่ายและมองเห็นภาพรวมของ วิธีการ/มาตรการ ในการป้องกันด้วย

กรณีศึกษา : Catch-Patch-Match

ท่ามกลางความหลากหลายของวิธีการ/มาตรการในการป้องกันทางไซเบอร์นั้น Australian Signal Directorate ระบุไว้ว่า มีสามวิธีปฏิบัติในการที่จะสามารถลดความเสี่ยงจากการได้รับอันตรายและความเสียหายอันเกิดจากการที่หน่วยงานถูกโจมตีลงได้ถึงอย่างน้อย ๘๕ % ดังนี้

Catch: Catch Malicious Application Software with a Whitelist

วิธีนี้ ให้หน่วยงานย่อยทำการวิเคราะห์ลักษณะงานทั้งหมดของและลำดับรายชื่อของ Application Software หรือลักษณะของ Application Software ที่ต้องการใช้ หลังจากนั้นรวบรวมส่งต่อไปยังหน่วยหน่วยงานใหญ่ เพื่อวิเคราะห์ถึง Application Software ที่ต้องการใช้ในภาพรวม พร้อมกำหนดชื่อของ Application Software ที่ผ่านการตรวจสอบแล้วว่าเป็น Application Software ที่ปลอดภัยและสามารถใช้ในภารกิจต่างๆ ตามความจำเป็นของทุกหน่วยงานย่อย แล้วจัดทำเป็นบัญชี Application Software ที่ปลอดภัย (Whitelist) กล่าวคือ จัดทำ Software Library ซึ่งระบุถึง Application Software เฉพาะที่ได้รับอนุญาตให้ทำการติดตั้งลงในเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายของหน่วยงานได้ ซึ่งวิธีนี้จะสามารถป้องกัน Application Software ประเภทแฝงมัลแวร์อันตรายที่อาจจะพยายามเข้ามาในระบบได้อย่างมีประสิทธิผล โดยในระดับนโยบายนั้น จะต้องมีการประกาศและบังคับใช้มาตรการการใช้งาน Application Software เฉพาะที่ระบุไว้ใน Whitelist อย่างเคร่งครัด

Patch: Patch Application Software and Operating System

วิธีนี้ หมายถึง Application Software (ที่มีระบุใน Whitelist) ที่ใช้งาน จะต้องมีการอัพเดท Software Patch ให้มีความเป็นปัจจุบันเสมอ เนื่องจากเวอร์ชั่นของ Patch ต่างๆ ที่ออกมานั้น จะมีการปรับปรุงและแก้ไขข้อบกพร่อง เช่น ช่องโหว่และ Bug ต่างๆ ที่พบหลังจากที่ Software มีการเปิดตัวใช้งาน ซึ่งผู้ไม่ประสงค์ดีจะใช้จุดอ่อนของช่องโหว่หรือ Bug ที่ตรวจพบ เพื่อประโยชน์ในการใช้เป็นช่องทางบุกรุกจู่โจม ดังนั้น การอัพเดท Patch จะทำให้การใช้งาน Application Software เกิดความปลอดภัยสูงสุดในเวลาปัจจุบันเสมอ ทั้งนี้ การออก Patch ใหม่และการอัพเดท อาจมีความห่างของช่วงเวลา (Time Gap) ได้ เนื่องจากผู้ใช้ยังไม่ทราบว่ามี Patch ใหม่นั้นๆ ออกมาแล้ว การทำให้ช่วงเวลาดังกล่าวมีความสั้นที่สุด (Minimization) จึงเป็นปัจจัยสำคัญที่ต้องตระหนักถึง โดยเฉพาะการอัพเดทในส่วนวิกฤติ (Critical Update) ซึ่งมักจะมีระบุไว้ในรายการอัพเดทให้ผู้ใช้ทราบด้วย

นอกเหนือจากการ Patch ในส่วนของ Application Software ให้เป็นปัจจุบันเสมอแล้ว ระดับความปลอดภัยสูงสุดของ Application Software จะอยู่บนพื้นฐานของการใช้ระบบปฏิบัติการ (Operating System) ที่มีการอัพเดทให้เป็นปัจจุบันมากที่สุดด้วย สิ่งสำคัญคือระบบปฏิบัติการใหม่ที่มีการอัพเดท Patch ครบถ้วน (Fully Patched) จะให้ระดับความปลอดภัยที่สูงกว่า Platform ที่เก่ากว่าเสมอ เช่น Microsoft Windows 10 ให้ระดับความปลอดภัยที่มากกว่า Windows 8, Windows 8 ให้ระดับความปลอดภัยที่มากกว่า Windows 7, Windows 7 ให้ระดับความปลอดภัยที่มากกว่า Windows Vista, Windows Vista ให้ระดับความปลอดภัยที่มากกว่า Windows XP, Windows XP ให้ระดับความปลอดภัยที่มากกว่า Windows 95 เป็นต้น ดังนั้นนอกจากการอัพเดท Patch ของระบบปฏิบัติการที่ใช้งานอยู่ให้มีความเป็นปัจจุบันจะมีความสำคัญอย่างยิ่งแล้ว การเปลี่ยนไปสู่การใช้งานระบบปฏิบัติที่ใหม่กว่า ก็เป็นอีกสิ่งหนึ่งที่จะให้ความคุ้มค่าในแง่ของระดับความปลอดภัยด้วย

Match: Match the Right People with the Right Privileges

วิธีนี้ หมายถึง สิทธิ์ในการเข้าถึงระดับผู้ดูแลระบบ (Administrative Privileges) จะต้องควบคุมและจำกัดเฉพาะกลุ่มบุคคลที่รับผิดชอบเท่านั้น นอกจากนี้ การระบุตัวตนและการ

พิสูจน์ทราบตัวตน (Identification & Authentication) จะต้องเป็นขั้นตอนที่มีความรัดกุม แข็งแกร่งและปลอดภัย ซึ่งโดยปกติแล้ว ผู้ไม่ประสงค์ดีที่เจาะระบบเข้ามา จะพยายามแสวงหาให้ได้มาซึ่งสิทธิ์แห่งความเป็นผู้ดูแลระบบ หรือพยายามไต่ระดับไปยังการได้รับสิทธิ์ที่สูงขึ้น เนื่องจากจะทำให้สามารถทำให้เข้าถึง (Access) ข้อมูลและทรัพยากรเครือข่ายได้มากขึ้น เพื่อการบรรลุประสงค์ในการโจมตี ดังนั้น การให้สิทธิ์และการจำกัดสิทธิ์แก่ผู้ใช้ในแต่ละระดับการปฏิบัติงาน จึงเป็นสิ่งจำเป็นอย่างยิ่งอีกสิ่งหนึ่งที่ผู้บริหารหน่วยงานจะต้องตระหนัก ซึ่งหน่วยงานที่ผู้ทำงานในระดับปฏิบัติสามารถมีสิทธิ์การเข้าถึงในระดับผู้ดูแลระบบหรือเสมือนเป็นเจ้าของเครื่องคอมพิวเตอร์ ซึ่งสามารถ เรียกดู แก้ไข ลบ เปลี่ยนแปลง ทุกสิ่งทุกอย่างได้ตามที่ต้องการ ก็ไม่ต่างอะไรกับการสร้างช่องโหว่ที่มีความอ่อนแอที่สุดในระบบ (Weakest Link)

กรณีตัวอย่างที่กำหนดนโยบายด้านความปลอดภัยของหน่วยงานด้วยกลยุทธ์ Catch-Patch-Match นั้น เมื่อวิเคราะห์อย่างละเอียดพบว่ามีความสอดคล้องในเชิงป้องกันการบุกรุกตามกระบวนการบุกรุก (Intrusion Process) ของภัยคุกคามจากการถูกแฮกอย่างมีนัยสำคัญ ดังนี้

Catch & Patch & Match: ป้องกันการเปิดช่องทางในการเชื่อมต่อเข้าสู่ระบบ (Code Execution)
Catch & Patch & Match: ป้องกันการขยายตัวเข้าไปในระบบเครือข่าย (Network Propagation)
Catch: ป้องกันการดึงข้อมูลสำคัญที่ต้องการ (Data Exfiltration)

ไม่มีการป้องใดที่ให้ระดับความปลอดภัยได้เต็ม ๑๐๐ % ทุกวิธีการหรือทุกมาตรการอาจจะต้องใช้ควบคู่กันเพื่อความปลอดภัยที่สูงขึ้น อย่างไรก็ตาม การวิเคราะห์ ๓ กลยุทธ์ Catch, Patch และ Match ดังกล่าว นับเป็นการสร้างภาพของความเข้าใจในองค์รวมของการโจมตี และการระวังป้องกัน แบบที่ให้ทั้งประสิทธิภาพและประสิทธิผลได้เป็นอย่างดี

บทที่ ๔
กฎหมายที่เกี่ยวข้องและจริยธรรมในการใช้เทคโนโลยีสารสนเทศ

ในการใช้งานระบบสารสนเทศของกำลังพล ทั้งการใช้งานระบบสารสนเทศของหน่วยงานตามปกติและการใช้งานที่มีส่วนเกี่ยวข้องกับระบบเครือข่ายสังคมออนไลน์ มีความจำเป็นที่จะต้องศึกษาและทำความเข้าใจกับกฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ตลอดจนจริยธรรมในการใช้งาน เพื่อให้การใช้งานระบบสารสนเทศเป็นไปอย่างเหมาะสม ดังนี้

๔.๑ กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ

กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศในประเทศไทยหลักๆ ประกอบด้วย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ (พ.ร.บ.คอมพิวเตอร์ ปี ๒๕๖๐) พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ (พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ ปี ๒๕๔๔) และกฎหมายลิขสิทธิ์ พ.ศ.๒๕๕๘ (พ.ร.บ.ลิขสิทธิ์ ปี ๒๕๕๘) รายละเอียดโดยสังเขป ดังนี้

๔.๑.๑ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐

พ.ร.บ.คอมพิวเตอร์ ปี ๒๕๖๐ นั้น ได้มีการปรับปรุงแก้ไขให้มีความทันสมัยและครอบคลุมมากยิ่งขึ้น โดยสรุปประเด็นได้ ดังนี้

๔.๑.๑.๑ การดูแลความเป็นส่วนตัว (Privacy) ของประชาชน ให้สามารถปฏิเสธการไม่รับสแปมได้ง่ายขึ้น พร้อมระบุเกณฑ์การพิจารณาสแปม รวมถึงการเข้าถึงข้อมูลของบุคคลอื่นโดยมิชอบ (มาตรา ๔, ๕, ๑๑)

๔.๑.๑.๒ การดูแลโครงสร้างพื้นฐานสำคัญของประเทศ (Critical Infrastructure) เช่น ระบบการเงิน การธนาคาร ระบบพลังงาน ไฟฟ้า ประปา และระบบสาธารณสุข เป็นต้น (มาตรา ๑๒)

๔.๑.๑.๓ การปรับปรุงความผิดฐานเผยแพร่ข้อมูล เพื่อเอาผิดต่อการฉ้อโกง ปลอมแปลง หรือข้อมูลอันเป็นเท็จ (มาตรา ๑๔ (๑))

๔.๑.๑.๔ การยกเว้นความผิดของผู้ให้บริการ เมื่อทำตามขั้นตอนตามกฎหมาย โดยกำหนดขั้นตอนการแจ้งเตือนการนำข้อมูลออกจากระบบคอมพิวเตอร์ เพื่อให้มีความชัดเจน เป็นไปในแนวทางที่ยอมรับได้ มีความโปร่งใส ตรวจสอบการดำเนินงานได้ (มาตรา ๑๕)

๔.๑.๑.๕ การดูแลความเสียหายต่อตัวบุคคล ที่รวมถึงการตัดต่อภาพของผู้เสียชีวิต และกำหนดข้อยกเว้นในการติชม ด้วยความเป็นธรรม (มาตรา ๑๖)

๔.๑.๑.๖ เพิ่มมาตรการบรรเทาความเสียหายสำหรับเนื้อหาที่ศาลพิพากษาว่าผิด โดยศาลอาจสั่งให้ทำลาย โฆษณาหรือเผยแพร่คำพิพากษา หรือใช้มาตรการอื่นๆ และสั่งให้ผู้ครอบครองข้อมูลนั้นตามหลักสิทธิที่จะถูกลืม (Right to be Forgotten) (มาตรา ๑๖/๑, ๑๖/๒)

๔.๑.๑.๗ เพิ่มมาตรการเปรียบเทียบในความผิดที่มีโทษสถานเบา ลดภาระของประชาชนในการดำเนินคดีในชั้นศาล เพื่อไม่ให้ติดอยู่ในกระบวนการยุติธรรมที่ต้องเสียเวลาและค่าใช้จ่าย (มาตรา ๑๗/๑)

๔.๑.๑.๘ การให้พนักงานเจ้าหน้าที่ที่เชี่ยวชาญ ให้ความช่วยเหลือทางเทคนิคแก่พนักงานเจ้าหน้าที่ตามกฎหมายอื่น เพื่อบรรเทาความเสียหายให้กับประชาชนโดยเร็วที่สุด (มาตรา ๑๘, ๑๙)

๔.๑.๑.๙ การพิจารณาขยายเวลาเก็บข้อมูลจราจรทางคอมพิวเตอร์ที่ใช้เป็นพยานหลักฐาน เนื่องจากเทคโนโลยีมีการเปลี่ยนแปลง และรูปแบบการกระทำความผิดมีความซับซ้อนมากขึ้น (มาตรา ๒๖)

โดยข้อสำคัญที่ผู้ปฏิบัติงานในหน่วยงานควรทราบ มีดังนี้

❒ ไม่ละเมิดการใช้งานคอมพิวเตอร์ของบุคคลอื่นที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต

❒ ไม่เจาะเข้าระบบคอมพิวเตอร์ โดยเฉพาะระบบที่อาจส่งผลต่อความมั่นคงของประเทศ และไม่เผยแพร่วิธีการ/มาตรการป้องกันการเข้าถึง ของระบบใดๆ

❒ ไม่เข้าถึงข้อมูลส่วนบุคคลของผู้อื่นที่เก็บเอาไว้ในระบบคอมพิวเตอร์

❒ ไม่ดักจับข้อมูลที่รับส่งในระบบคอมพิวเตอร์

❒ ไม่ตัดต่อ ทำลาย แก้ไข เปลี่ยนแปลงข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาต

❒ ไม่แพร่กระจายไวรัสหรือมัลแวร์เข้าสู่ระบบคอมพิวเตอร์ของผู้อื่น

❒ ไม่ส่งสแปมหรือโฆษณาต่างๆ ไปสร้างความรำคาญให้ผู้อื่น

❒ ไม่สร้างโปรแกรมหรือซอฟต์แวร์เพื่อสนับสนุนผู้กระทำความผิด

❒ ไม่นำเข้า จัดเก็บ หรือเผยแพร่ภาพลามกอนาจาร หรือข้อมูลอันเป็นเท็จ หรือก่อให้เกิดความตื่นตระหนกต่อประชาชน

สรุปประมวลความผิดโดยสังเขปที่ผู้ปฏิบัติงานในหน่วยงานควรทราบ มีดังนี้

❒ การทำลาย แก้ไข ไม่ว่าทั้งหมดหรือบางส่วนของข้อมูลคอมพิวเตอร์ผู้อื่น มีโทษจำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑๐๐,๐๐๐ บาท

❒ การระงับ ชะลอ ขัดขวาง รบกวนระบบของผู้อื่นจนไม่สามารถทำงานตามปกติได้ โทษปรับไม่เกิน ๑๐๐,๐๐๐ บาท

❒ การโพสต์ข้อมูลที่บิดเบือน หรือปลอม จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑๐๐,๐๐๐ บาท

❒ การโพสต์ข้อมูลเท็จที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศ ความปลอดภัยสาธารณะ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ หรือทำให้เกิดความตื่นตระหนกแก่ประชาชน จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑๐๐,๐๐๐ บาท

❒ การโพสต์ข้อมูลเกี่ยวกับความมั่นคงแห่งราชอาณาจักร-การก่อการร้าย จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑๐๐,๐๐๐ บาท

❒ ผู้ดูแลระบบที่เปิดให้มีการแสดงความคิดเห็น เมื่อพบเนื้อหาที่ผิดกฎหมาย ถ้าได้รับการแจ้งเตือนแล้วลบออกไม่ต้องรับโทษ แต่ถ้าไม่ยอมลบออก โทษจำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑๐๐,๐๐๐ บาทหรือทั้งจำทั้งปรับ

❒ การแก้ไขเปลี่ยนแปลงทำให้ระบบทำงานไม่ปกติ ทำให้บาดเจ็บ ทรัพย์สินเสียหาย โทษจำคุกไม่เกิน ๑๐ ปี ปรับไม่เกิน ๒๐๐,๐๐๐ บาท

❒ การโพสต์ภาพลามกอนาจารและสามารถแชร์สู่ประชาชนคนอื่นได้ จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑๐๐,๐๐๐ บาท

❒ การโพสต์ภาพของผู้อื่นที่เกิดจากการสร้าง ตัดต่อ หรือดัดแปลง ที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง มีโทษจำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๒๐๐,๐๐๐ บาท

❒ การโพสต์ภาพผู้เสียชีวิต หากเป็นการโพสต์ที่ทำให้บิดามารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่นเกลียดชัง หรือได้รับความอับอาย มีโทษจำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๒๐๐,๐๐๐ บาท

๔.๑.๒ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔

พ.ร.บ.ธุรกรรมทางอิเล็กทรอนิกส์ ปี ๒๕๔๔ ได้กล่าวถึงประเด็นพิจารณาเกี่ยวกับเอกสารอิเล็กทรอนิกส์ที่สำคัญที่ผู้ปฏิบัติงานในหน่วยงานควรทราบ ดังนี้

๔.๑.๒.๑ ศาลจะยอมรับกระบวนการพิสูจน์และยืนยันทางอิเล็กทรอนิกส์ของเอกสารอิเล็กทรอนิกส์ ที่สามารถพิสูจน์ได้ด้วยกระบวนการและหลักการน่าที่เชื่อถือได้ ซึ่งหมายถึงกระบวนการตรวจยืนยันความถูกต้องครบถ้วนของเอกสาร (Data Integrity) ด้วยวิธีการสร้างชุดตัวแทนข้อมูล (Message Digest) และกระบวนการลงลายมือชื่อดิจิทัล (Digital Signature) ที่ป้องกันการปฏิเสธความรับผิดชอบ (Non-Repudiation) สามารถนำไปพิสูจน์ความถูกต้องและความเป็นเจ้าของในชั้นศาลได้ หากเป็นไปตามเทคโนโลยีเกี่ยวข้องอย่างถูกต้อง

๔.๑.๒.๒ วันเวลาที่ทำธุรกรรมทางอิเล็กทรอนิกส์ให้ถือว่ามีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้ามาสู่ระบบข้อมูลของผู้รับข้อมูล หากผู้รับข้อมูลได้กำหนดระบบข้อมูลที่ประสงค์จะใช้ในการรับข้อมูลอิเล็กทรอนิกส์ไว้โดยเฉพาะ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ข้อมูลอิเล็กทรอนิกส์นั้นได้เข้าสู่ระบบข้อมูลที่ผู้รับข้อมูลได้กำหนดไว้นั้น แต่ถ้าข้อมูลอิเล็กทรอนิกส์ดังกล่าวได้ส่งไปยังระบบข้อมูลอื่นของผู้รับข้อมูลซึ่งมิใช่ระบบข้อมูลที่ผู้รับกำหนดไว้ ให้ถือว่าการรับข้อมูลอิเล็กทรอนิกส์มีผลนับแต่เวลาที่ได้เรียกข้อมูลอิเล็กทรอนิกส์จากระบบข้อมูลนั้น

๔.๑.๓ กฎหมายลิขสิทธิ์ พ.ศ.๒๕๕๘

กฎหมายลิขสิทธิ์ ปี ๒๕๕๘ ได้กล่าวถึงประเด็นพิจารณาเกี่ยวกับลิขสิทธิ์ของผลงานทางอิเล็กทรอนิกส์ที่สำคัญที่ผู้ปฏิบัติงานในหน่วยงานควรทราบ ดังนี้

๔.๑.๓.๑ ให้การคุ้มครองลิขสิทธิ์ของเจ้าของลิขสิทธิ์ผลงานทางอิเล็กทรอนิกส์ เช่น สิทธิในการทำซ้ำหรือดัดแปลงงาน การเผยแพร่งานต่อสาธารณชน และให้เช้าต้นฉบับหรือสำเนาผลงานบางประเภท

๔.๑.๓.๒ ข้อยกเว้นการละเมิดลิขสิทธิ์ผลงานทางอิเล็กทรอนิกส์ทั่วไป ให้สามารถนำข้อมูลของผู้อื่นมาใช้ได้โดยไม่ต้องขออนุญาต โดยพิจารณาจาก ๔ ปัจจัย ดังนี้

๑) ลักษณะการนำไปใช้มิใช่เป็นเชิงพาณิชย์

๒) ข้อมูลเป็นข้อเท็จจริงอันเป็นสาธารณประโยชน์ ซึ่งทุกคนสามารถนำไปใช้ได้

๓) จำนวนเนื้อหาที่จะคัดลอกไปใช้เมื่อเป็นสัดส่วนกับข้อมูลที่เป็นลิขสิทธิ์ทั้งหมด

๔) ผลกระทบของการนำข้อมูลไปใช้ที่มีต่อความเป็นไปได้ทางการตลาดหรือคุณค่าของงานที่มีลิขสิทธิ์นั้น

๔.๑.๓.๓ ข้อยกเว้นการละเมิดลิขสิทธิ์ที่เกี่ยวกับโปรแกรมคอมพิวเตอร์ โดยมิให้ถือว่าละเมิดลิขสิทธิ์ หากไม่มีวัตถุประสงค์เพื่อแสวงหาผลกำไรในกรณีดังนี้

๑) วิจัยหรือศึกษาโปรแกรมคอมพิวเตอร์นั้น

๒) ใช้เพื่อประโยชน์ของเจ้าของสำเนาโปรแกรมคอมพิวเตอร์นั้น

๓) ติชม วิจารณ์ หรือแนะนำผลงานโดยมีการรับรู้ถึงความเป็นเจ้าของลิขสิทธิ์ในโปรแกรมคอมพิวเตอร์นั้น

๔) เสนอรายงานข่าวทางสื่อสารมวลชนโดยมีการรับรู้ถึงความเป็นเจ้าของลิขสิทธิ์ในโปแกรมคอมพิวเตอร์นั้น

๕) ทำสำเนาโปรแกรมคอมพิวเตอร์ในจำนวนที่สมควร โดยบุคคลผู้ซึ่งได้ซื้อหรือได้รับโปรแกรมนั้นมาจากบุคคลอื่นโดยถูกต้อง เพื่อเก็บไว้ใช้ประโยชน์ในการบำรุงรักษาหรือป้องกันการสูญหาย

๖) ทำซ้ำ ดัดแปลง นำออกแสดง หรือทำให้ปรากฏเพื่อประโยชน์ในการพิจารณาของศาลหรือเจ้าพนักงานซึ่งมีอำนาจตามกฎหมาย หรือในการรายงานผลการพิจารณาดังกล่าว

๗) นำโปรแกรมคอมพิวเตอร์นั้นมาใช้เป็นส่วนหนึ่งในการถามและตอบในการสอบ

๘) ดัดแปลงโปรแกรมคอมพิวเตอร์ในกรณีที่จำเป็นต่อการใช้

๙) จัดทำสำเนาโปรแกรมคอมพิวเตอร์เพื่อเก็บรักษาไว้สำหรับอ้างอิง หรือค้นคว้าเพื่อประโยชน์ของสาธารณชน

๔.๒ จริยธรรมในการใช้เทคโนโลยีสารสนเทศ

การใช้งานเทคโนโลยีสารสนเทศ มีความจำเป็นต้องระมัดระวังไม่ให้ละเมิดต่อกฎหมายในทุกมิติ ในขณะเดียวกัน การใช้งานเทคโนโลยีสารสนเทศก็มีความจำเป็นที่จะต้องปฏิบัติให้มีความเหมาะสม ถูกต้องตามทำนองคลองธรรม สอดคล้องกับวัฒนธรรม ประเพณี และมารยาทอันดีงามของสังคม ดังนั้น ผู้ปฏิบัติงานในหน่วยงาน จึงควรต้องตระหนักถึงจริยธรรมในการใช้เทคโนโลยีสารสนเทศ ใน ๔ ประเด็นหลัก ดังนี้

๔.๒.๑ ไม่ละเมิดความเป็นส่วนตัวของผู้อื่น

๔.๒.๒ ไม่บิดเบือนข้อมูลให้ผิดไปจากความเป็นจริง

๔.๒.๓ ไม่ละเมิดสิทธิความเป็นเจ้าของ

๔.๒.๔ ไม่เข้าถึงข้อมูลของบุคคลอื่นโดยไม่ได้รับอนุญาต

นอกจากนี้ ในการใช้งานสื่อสังคมแบบออนไลน์ของผู้ปฏิบัติงานในหน่วยงาน ควรตระหนักและใส่ใจในการปฏิบัติให้เหมาะสม ดังนี้

❒ ไม่โพสต์หรือส่งต่อข้อความ รูป หรือคลิปวิดีโอ ที่อาจส่งผลทำร้าย ให้ร้าย หรือสร้างความเสียหายแก่ผู้อื่น หรือเป็นการต่อว่า/เสียดสี/พาดพิงถึงผู้อื่นในเชิงลบ ทั้งแบบกลุ่มและแบบสาธารณะ

❒ ไม่ส่งข้อมูลในลักษณะที่สร้างความรบกวนแก่ผู้อื่น (รูปแบบข้อมูล, ปริมาณข้อมูล) ที่มิใช่กลุ่มปิดหรือมีเฉพาะสมาชิกที่สมัครใจ เช่น โฆษณาเสนอขายสินค้า ส่งต่อข้อมูลครั้งละมากๆ จดหมายลูกโซ่ เมลขยะ

❒ ไม่ติดตามหรือสอดส่องข้อมูลตลอดจนกิจกรรมของผู้อื่นเพื่อการจับผิด กล่าวโทษ หรือเพื่อสร้างความเกลียดชัง ชิงชัง หรือก่อให้เกิดความรู้สึกในแง่ลบ

❒ ไม่ขโมยข้อมูล หรือนำข้อมูลไปใช้โดยไม่อ้างอิงแหล่งที่มา

❒ ไม่สร้างพยานเท็จ หรือหลักฐานเท็จ

❒ ไม่แอบอ้างใช้ชื่อของผู้อื่น หรือใช้บัญชีผู้ใช้งานของผู้อื่น และไม่ใช้สื่อสังคมออนไลน์แบบกลุ่มในลักษณะที่ไม่ถูกต้องเหมาะสม

❒ คำนึงถึงผลกระทบต่อเนื่องทางสังคมที่อาจจะเกิดขึ้นทุกครั้ง

❒ คำนึงถึงการเคารพผู้อื่นและการเคารพสิทธิของผู้อื่นทุกครั้ง

บรรณานุกรม

Abet Dela Cruz. **The "Catch-Patch-Match strategy"**. [Online]. (January 18, 2017). Available from: http://www.manilatimes.net/catch-patch-match-strategy/307487/ [April 1, 2018]

Australian Signals Directorate. **Strategies to Mitigate Cyber Security Incidents**. [Online]. (February 1, 2017). Available from: https://asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm [March 1, 2018]

สำนักงานรัฐบาลอิเล็กทรอนิกส์ (องค์การมหาชน). **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560: ที่มาและสาระสำคัญ** (PDF). [Online]. Available from: https://www.ega.or.th/upload/download/file_ce8c32197b28a5d438136a3bd8252b7c.pdf [March 1, 2018]

Bellare M. and Rogaway P. **Introduction to Modern Cryptography**. (Lecture Notes for Cryptography Course at the University of California at Sandiego. [Online]. (September 21, 2005). Available from: http://cseweb.ucsd.edu/~mihir/cse207/classnotes.html) [March 1, 2018]

Christof Paar, Jan Pelzl and Bart Preneel. **Understanding Cryptography: A Textbook for Students and Practitioners**. Springer (2010). p. 7.

Gary C. Kessler. **An Overview of Cryptography**. [Online]. (May 22, 2011). Available from: http://www.garykessler.net/library/crypto.html [March 1, 2018]

เจ้าของผลงาน

ยศ-ชื่อ-ชื่อสกุล นาวาอากาศเอก ณัฐวุฒิ สามไพบูลย์

คุณวุฒิ

การศึกษาทั่วไป

- ปริญญาตรี
  Software Engineering, National Defense Academy, ประเทศญี่ปุ่น
- ปริญญาโท
  Mathematical Computing and Operations Research, National Defense Academy, ประเทศญี่ปุ่น
- ปริญญาเอก
  Computer Science and Information Management, Asian Institute of Technology (AIT)

การศึกษาทางทหาร

- โรงเรียนนายร้อยรวมเหล่า, ประเทศญี่ปุ่น
- โรงเรียนอบรมนายทหารสัญญาบัตร, NARA, ประเทศญี่ปุ่น
- โรงเรียนนายทหารชั้นผู้บังคับฝูง, กรมยุทธศึกษาทหารอากาศ
- โรงเรียนเสนาธิการทหารอากาศ, กรมยุทธศึกษาทหารอากาศ
- วิทยาลัยการทัพอากาศ (Air War College), Japan Air Self-Defense Force, ประเทศญี่ปุ่น
- วิทยาลัยเสนาธิการทหารร่วม (Joint Staff College), กระทรวงกลาโหม, ประเทศญี่ปุ่น

ตำแหน่ง รองผู้อำนวยการกองสงครามไซเบอร์
สำนักระบบบัญชาการและควบคุม
กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

โทรศัพท์ ๒ – ๐๖๕๗, ๐๙ - ๖๘๕๙ - ๗๐๙๑

สรุปสาระสำคัญของบทความทางวิชาการ

๑. ชื่อของบทความทางวิชาการ

ภาษาไทย ความรู้ที่สำคัญด้านการรักษาความปลอดภัยสำหรับกำลังพลที่ใช้งานระบบสารสนเทศ
ภาษาอังกฤษ (ถ้ามี) -

๒. ประเภทของผลงาน

☑ บทความทางวิชาการ
❒ บทความทางวิชาการที่แปลมาจากภาษาต่างประเทศ

๓. ผลงานนี้เกี่ยวข้องกับสายวิทยาการใด

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ

๔. ให้ระบุข้อมูลของสาระสำคัญโดยย่อดังต่อไปนี้

๔.๑ ที่มาหรือแรงจูงใจที่ทำให้เกิดความคิดในการเขียนบทความทางวิชาการ

กำลังพลกองทัพอากาศ ที่ใช้งานระบบสารสนเทศทั้งระบบและอุปกรณ์ของกองทัพอากาศ, ระบบและอุปกรณ์ส่วนบุคคลที่มีการเชื่อมต่อหรือใช้งานร่วมกับระบบและอุปกรณ์ของกองทัพอากาศ และการใช้งานเครือข่ายสังคมออนไลน์ของกำลังพล โดยภาพรวม ยังมีความรู้เกี่ยวกับภัยคุกคามและความตระหนักรู้ด้านการรักษาความปลอดภัยในการใช้งานระบบสารสนเทศทั้งมวลที่ไม่เพียงพอและไม่ครอบคลุม ซึ่งการยกระดับการรักษาความปลอดภัยแบบบูรณาการของกำลังพล ภายใต้ความรู้และความตระหนักรู้ที่ถูกต้องและเหมาะสม จะส่งผลให้ระดับของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองทัพอากาศในภาพรวมสูงขึ้นและมีความปลอดภัยเพิ่มมากขึ้น สามารถสนองตอบต่อภารกิจภายใต้การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางได้อย่างมีประสิทธิภาพและประสิทธิผลที่สูงขึ้น

ผู้จัดทำจึงได้เขียนบทความทางวิชาการเรื่องความรู้ที่สำคัญด้านการรักษาความปลอดภัยสำหรับกำลังพลที่ใช้งานระบบสารสนเทศขึ้นจากประสบการณ์และความรู้ โดยได้พิจารณาให้ครอบคลุมมิติสำคัญซึ่งกำลังพลควรทราบและเป็นประโยชน์ต่อการรักษาความปลอดภัยในการใช้งานระบบสารสนเทศอย่างบูรณาการ โดยได้ครอบคลุมองค์ความรู้เกี่ยวกับระบบสารสนเทศในด้านขององค์ประกอบที่เกี่ยวข้องและคุณสมบัติด้านความปลอดภัยของระบบสารสนเทศ รวมถึงภัยคุกคามทางไซเบอร์ทั้งรูปแบบเดิมและรูปแบบใหม่ที่พบปัจจุบัน พร้อมแนวทางในการป้องกัน

นอกจากนี้ ยังได้วิเคราะห์ถึงกำลังพลผู้ใช้งานระบบสารสนเทศ (Peopleware) กับการรักษาความปลอดภัย, รหัสผ่าน (Password) และความปลอดภัย, การบูรณาการอุปกรณ์คอมพิวเตอร์และการสื่อสารส่วนบุคคลมาใช้ร่วมกับระบบสารสนเทศของกองทัพอากาศ (BYOD) และการใช้บริการจัดเก็บข้อมูลบน Cloud Services กับการรักษาความปลอดภัย พร้อมทั้งได้แนะนำเทคโนโลยีด้านความปลอดภัยในปัจจุบันที่สำคัญและควรทราบ ได้แก่ การพิสูจน์ยืนยันตัวตนแบบพหุปัจจัย (Multi-factor Authentication), การลงลายมือชื่อดิจิทัล (Digital Signature) และเทคโนโลยี Blockchain

พร้อมกันนี้ ได้เสนอแนะแนวทางและวิธีการในการกำหนดนโยบายด้านความปลอดภัยของหน่วยงาน โดยยกตัวอย่างกรณีศึกษา Catch-Patch-Match ของ Australian Signal Directorate,

Department of Defence ซึ่งเป็นตัวอย่างนโยบายด้านการรักษาความปลอดภัยอันทรงประสิทธิผลที่มีการประกาศเพื่อเป็นแนวทางกลยุทธ์ในการป้องกันภัยคุกคามทางไซเบอร์ให้กับทั้งองค์กรภาครัฐและเอกชนของประเทศออสเตรเลีย นอกจากนี้ ยังได้ประมวลองค์ความรู้ด้านกฎหมายที่เกี่ยวข้องและจริยธรรมในการใช้งานระบบสารสนเทศที่สำคัญไว้ด้วย เพื่อมุ่งหมายให้เป็นเอกสารประกอบในการเสริมสร้างความรู้และความตระหนักรู้ด้านการรักษาความปลอดภัยในการใช้งานระบบสารสนเทศแบบบูรณาการหลายมิติ ให้แก่กำลังพลของกองทัพอากาศ

๔.๒ ลักษณะของบทความทางวิชาการ

☑ เป็นผลงานที่เขียนขึ้นโดยใช้ความรู้และประสบการณ์

❒ เป็นผลงานที่ได้รวบรวมและเรียบเรียงขึ้น

❒ เป็นผลงานที่ได้แปลขึ้น

๔.๓ เคยได้รับรางวัลอันดับที่ - จาก -

❒ เป็นเงินรางวัล จำนวน - เมื่อ -

❒ เป็นของรางวัล - เมื่อ -

๔.๔ กองทัพอากาศได้รับประโยชน์และผลกระทบจากผลงานนี้อย่างไร

มีเอกสารสำหรับใช้ประกอบในการเสริมสร้างความรู้และความตระหนักรู้ด้านการรักษาความปลอดภัยในการใช้งานระบบสารสนเทศแบบหลายมิติ ที่มีความเป็นปัจจุบัน ให้แก่กำลังพลกองทัพอากาศ

๔.๕ มีการรับรองผลงานไปใช้ประโยชน์หรือไม่

☑ ไม่มี

❒ มี รายละเอียดตามเอกสารอ้างอิงที่แนบ จำนวน - แผ่น

๔.๖ งบประมาณที่ใช้ในการจัดทำต่อหน่วย

❒ จำนวนเงิน - บาท

❒ แหล่งที่ได้รับงบประมาณ -

๔.๗ มีการเผยแพร่ผลงานนี้หรือไม่

❒ มี โดยวิธี - ที่ใด - เมื่อ -

☑ ไม่มี (ผลงานเต็มรูปเล่มของบทความทางวิชาการสำหรับกองทัพอากาศฉบับนี้ยังไม่เคยเผยแพร่ที่ใด)

๔.๘ อื่น ๆ (ถ้ามี) บางส่วนของบทความทางวิชาการฉบับนี้ ได้รับการตีพิมพ์ในนิตยสารแทงโก้ (Tango Magazine) และหนังสือข่าวทหารอากาศ และบางส่วนของบทความทางวิชาการนี้ ได้รับการนำไปประกอบเอกสารตำราเรียนในส่วนของด้านเทคโนโลยีสารสนเทศและการรักษาความปลอดภัยของมหาวิทยาลัยสุโขทัยธรรมาธิราช

๕. รายชื่อผู้ร่วมงาน

นาวาอากาศเอก ณัฐวุฒิ สามไพบูลย์ (เจ้าของผลงาน)