(Special Article)

Identity Theft : The Threat of Cyber Worlds in the 21st Century

Supon Phrommaphan

Department of Business Computer, School of Information Technology, Sripatum University

*Correspondence to : *supon.ph@spu.ac.th, **preecha.ta@spu.ac.th*

At present, the threat of internet users there appears to be more in order, due to the increasing number of users leaping, In which the number of these people is both good and bad, mixed together. For bad people, causing damage to others and other organizations by acting as a threat in many different ways, such as stealing other people's identities Which is a terrible threat in the present condition. Identity theft is self characteristics, Including information used to identify Information for communication or use to search for people or is information shared with other information to identify individuals or also known as personal information the following example is what identifies as identity: full name, surname of mother before marriage, address, date of birth, place of birth, genetic information, ID card number, Social Security Number, Driver's license number Vehicle registration number, Passport number, credit card number, Phone number, face, iris, fingerprint, fingerprint, signature etc.

Keywords : Identity theft, Social media, e-Commerce, Personal information, Phishing, Spyware

Royal Thai Air Force Medical Gazette, Vol. 65 No. 1 January - April 2019

(บทความพิเศษ)

การขโมยอัตลักษณ์ : ภัยคุกคามแห่งโลกไซเบอร์ในศตวรรษที่ 21

สุพล พรหมมาพันธุ์

คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

ในปัจจุบันภัยคุกคามของผู้ใช้อินเทอร์เน็ต มีปรากฏให้เห็นมากขึ้นเป็นลำดับ เนื่องจากมีจำนวนผู้ใช้เพิ่มมากขึ้นอย่างก้าวกระโดด ซึ่งในจำนวนบุคคลเหล่านี้มีทั้งคนดีและไม่ดีปะปนกันไป สำหรับคนที่ไม่ดีได้สร้างความเดือดร้อนเสียหายให้กับผู้อื่นและองค์กรอื่น ๆ โดยการกระทำตนให้เป็นภัยคุกคามในลักษณะต่าง ๆ มากมาย เช่น การขโมยอัตลักษณ์ของบุคคลอื่น ซึ่งเป็นภัยคุกคามที่น่ากลัวในสภาพปัจจุบัน การขโมยอัตลักษณ์ (Identity Theft) คือการขโมยลักษณะเฉพาะตัว ได้แก่ ข้อมูลที่ใช้ระบุตัวตน ข้อมูลใช้ในการติดต่อสื่อสาร หรือใช้ค้นหาบุคคล หรือเป็นข้อมูลที่ใช้ร่วมกับข้อมูลอื่นเพื่อระบุตัวบุคคล หรือเรียกอีกอย่างหนึ่งว่า ข้อมูลส่วนบุคคล ตัวอย่างต่อไปนี้ คือ สิ่งที่ระบุว่าเป็นอัตลักษณ์ ได้แก่ ชื่อเต็ม นามสกุลของมารดาก่อนแต่งงาน ที่อยู่ วัน เดือน ปีเกิด สถานที่เกิด ข้อมูลพันธุกรรม หมายเลขบัตรประจำตัวประชาชน หมายเลขบัตรประกันสังคม หมายเลขใบอนุญาตขับขี่ หมายเลขทะเบียนยานพาหนะ หมายเลขหนังสือเดินทาง (Passport) หมายเลขบัตรเครดิต เบอร์โทรศัพท์ ใบหน้า ม่านตา ลายพิมพ์นิ้วมือ ลายมือ ลายเซ็น เป็นต้น

คำสำคัญ : การขโมยอัตลักษณ์, สื่อสังคมออนไลน์, พาณิชย์อิเล็กทรอนิกส์, ข้อมูลส่วนบุคคล, การหลอกลวงทางอินเทอร์เน็ต, สปายแวร์

ปัจจุบันอินเทอร์เน็ตได้รับความนิยมเป็นอย่างมาก โดยมีผู้ใช้อินเทอร์เน็ต และ Social Media ทั่วโลกประจำปี 2017 ที่เก็บข้อมูลโดย We Are Social ดิจิทัลเอเจนซี่ในประเทศสิงคโปร์และ Hootsuite ทั้งนี้ ข้อมูลทั้งหมดมาจาก 238 ประเทศทั่วโลก รวมถึงประเทศไทยด้วย คือ ข้อมูลเบื้องต้นของประชากรทั่วโลกในปี 2017 ประชากรทั่วโลกมีจำนวน 7,476 พันล้านคน มีผู้ใช้อินเทอร์เน็ตทั่วโลก 3,773 ล้านคน คิดเป็น 50 % ผู้ใช้ Social Media 2,789 ล้านคน คิดเป็น 37 % ผู้ใช้โทรศัพท์มือถือ 4,917 ล้านคน คิดเป็น 66 % ผู้ใช้ Social Media ผ่านโทรศัพท์มือถือ 2,549 ล้านคน คิดเป็น 34 % ส่วนการเข้าถึงอินเทอร์เน็ตเมื่อแบ่งตามอุปกรณ์ (Device) คือ แล็บท็อป และเดสก์ทอป 45 % ลดลงจากปีที่ผ่านมา 20 % สมาร์ทโฟน 50 % เพิ่มขึ้นจากปีที่ผ่านมา 30 % แท็บเล็ต 5 % ลดลงจากปีที่ผ่านมา 5 % และอุปกรณ์อื่น ๆ 0.12 % เพิ่มขึ้นจากปีที่ผ่านมา 33 % สำหรับผู้ใช้ Social Media ทั่วโลก 2,789 ล้านคน คิดเป็น 37 % จากจำนวนประชากรทั่วโลกใช้ Social Media ผ่านมือถือ 2,549 ล้านคน คิดเป็น 34 % จากจำนวนประชากรทั่วโลก ส่วนทวิตเตอร์ผู้ที่นิยมใช้ส่วนใหญ่เป็นกลุ่มวัยรุ่นหนุ่มสาว WeChat เป็นแอพลิเคชั่นที่ได้รับความนิยมมากในประเทศจีน และ WhatsApp นิยมใช้ในยุโรปและอเมริกา LinkedIn คนนิยมใช้เกี่ยวกับการทำงาน หรือหางาน หรือใช้เขียน Profile Professional เช่น ประวัติการศึกษาประสบการณ์ในการทำงาน ซึ่งคล้ายคลึงกับการเขียน Resume Online ในแต่ละประเทศมีการใช้ Social Media แตกต่างกัน ขึ้นอยู่กับวัฒนธรรมของแต่ละประเทศ เช่น ในประเทศไทยจะมีการใช้เฟซบุ๊คกันมากที่สุด และนิยมใช้เพื่อการแชร์รูปภาพ วิดีโอ การ Comments ต่าง ๆ

รูปภาพที่ 1 ข้อมูลผู้ใช้อินเทอร์เน็ตทั่วโลกในปี 2017 (Sources: http://wearesocial.com)

การเข้าถึงอินเทอร์เน็ตของคนไทย คนไทยเข้าถึงอินเทอร์เน็ต 67 % จากจำนวนประชากรทั้งหมดเติบโต 21 % เมื่อเทียบกับช่วงเวลาเดียวกันของปีที่แล้ว ทำให้ตอนนี้ประเทศไทยอยู่ในลำดับที่ 18 ทั้งนี้ ค่าเฉลี่ยการเข้าถึงอินเทอร์เน็ตของประชากรทั่วโลก อยู่ที่ 50 % คนไทยใช้เวลาเล่นอินเทอร์เน็ตผ่านแล็บท็อป/เดสก์ทอป 4.35 ชั่วโมงต่อวัน ซึ่งมากกว่าบนสมาร์ทโฟน โดยมีเวลาเฉลี่ยอยู่ที่ 4.14 ชั่วโมงต่อวัน คนไทยใช้สมาร์ทโฟนเข้าเว็บไซต์เป็นอันดับ 5 จากประเทศที่สำรวจทั้งหมด อยู่ที่ 66 % ทั้งนี้ ค่าเฉลี่ยของประชากรทั่วโลกที่ใช้สมาร์ทโฟนเข้าเว็บไซต์อยู่ที่ 50 % คนไทยใช้ Social Media มากเป็นอันดับ 7 ของโลก ด้วยสัดส่วน 67 % จากจำนวนประชากรทั้งหมดในประเทศ คนไทยใช้เวลากับ Social Media เฉลี่ยวันละ 2.48 ชั่วโมง อยู่ในลำดับที่ 12 ของโลก ที่มีผู้คนใช้มากได้แก่ กรุงเทพฯ เชียงใหม่ และภูเก็ต ข้อมูลเกี่ยวกับ Facebook ปัจจุบัน Facebook มียอดผู้ใช้งานต่อเดือน 1,871 ล้านคน ในจำนวนนั้น 87 % ใช้งานผ่านมือถือ 55 % ใช้งานทุกวัน เมื่อแบ่งตามเพศ พบว่าผู้ชายใช้ Facebook มากกว่าผู้หญิง คนไทยใช้ Facebook เป็นอันดับ 8 ของโลก ด้วยจำนวน 46,000,000 คน ผู้ใช้ Facebook ส่วนใหญ่ 80 % ใช้งานผ่านสมาร์ทโฟนตามมาด้วยแล็บท็อป และเดสก์ทอป 39 %, แท็บเล็ต 11 % และฟีเจอร์โฟน 1 %

นอกจากนี้ ยังมีข้อมูลเกี่ยวกับการซื้อขายสินค้าพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) จำนวนผู้ซื้อสินค้าผ่านระบบ E-Commerce มีทั้งหมด 1,610 ล้านคน คิดเป็น 22 % ของประชากรทั่วโลก มูลค่ารวม 1,915,000,000,000 ดอลล่าร์ เฉลี่ยต่อคนอยู่ที่ 1,189 ดอลล่าร์ ประเทศไทยมีผู้ซื้อของผ่านระบบ E-Commerce ในรอบเดือนที่ผ่านมา 51 % อยู่ในลำดับที่ 15 ในส่วนของการซื้อสินค้าออนไลน์ผ่านสมาร์ทโฟน ประเทศที่มีสัดส่วนมากที่สุดคือ เกาหลีใต้ 55 % ส่วนประเทศไทย อยู่ในลำดับที่ 3 มี 41 % เมื่อเทียบกับช่วงเวลาเดียวกันของปีที่แล้ว ไทยเติบโตขึ้น 60 % เฉลี่ยค่าใช้จ่ายต่อคนอยู่ที่ 212 ดอลล่าร์ (ประมาณ 7,434 บาท) (Sources: https//www.marketingoops.com และ http://wearesocial.com)

จากตัวเลขผู้ใช้อินเทอร์เน็ต การใช้ Social Media รวมไปถึงการซื้อขายสินค้าพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) เป็นแนวโน้มที่เติบโตขึ้นอย่างต่อเนื่อง ซึ่งเป็นโอกาสของผู้ที่ต้องการทำธุรกิจเป็นอย่างยิ่งในการหาช่องทางขายสินค้า การทำตลาดผ่านระบบดิจิทัล (Digital Marketing) เป็นแนวโน้มที่ยิ่งมาแรง เพราะมีต้นทุนที่ไม่แพงเหมือน

การทำตลาดในสื่อระบบเดิม มีหลักการที่สำคัญ (1) The New – Multi Screen World หมายถึงว่า ในปัจจุบัน ผู้ใช้ 1 คน มีอุปกรณ์หลายชนิด เช่น สมาร์ทโฟน แท็บเล็ต โน้ตบุ๊ค คอมพิวเตอร์ เป็นต้น ในเว็บไซต์ www.daydev.com ได้รายงานวิเคราะห์การใช้งาน Multi-Screen เทรนด์พฤติกรรมผู้บริโภคจาก Google ซึ่งแสดงให้เห็นว่า การทำการตลาดในปัจจุบันนี้นั้น 90 % ของโอกาสที่กลยุทธ์ของบริษัทที่จะสำเร็จนั้น ขึ้นอยู่กับอุปกรณ์หรือ Devices ของผู้บริโภคด้วย และโอกาสที่เป็นไปได้มากที่สุด คือช่วงเวลาของการเดินทาง และการเดินทางก็จะมีผลต่อการใช้งานอุปกรณ์สื่อสาร เพราะว่ายุคนี้ผู้บริโภคเช็คอีเมลจากสมาร์ทโฟน แท็บเล็ต ระหว่างที่เดินทางอยู่บนรถไฟ รถไฟฟ้า รถโดยสารระหว่าง บ้านไปยังที่ทำงาน (2) การทำการตลาดผ่านเครื่องมือการค้นหาบนอินเทอร์เน็ต (Search Engine Marketing: SEM) สามารถแยกย่อยออกเป็น 2 รูปแบบ คือ 1) การปรับแต่งการค้นหา (Search Engine Optimization: SEO) ได้แก่การโปรโมทเว็บไซต์ เพื่อเพิ่มอันดับของเว็บไซต์ในส่วนของผลการค้นหาทั่วไปในหน้า Search Result Page โดยการปรับเปลี่ยนโครงสร้างภายในเว็บไซต์ให้เป็นไปตามกฎของการค้นหาและการเพิ่ม Backlinks ที่มีคุณภาพมายังเว็บไซต์ 2) การจ่ายต่อคลิก (Pay Per Click: PPC) คือ ส่วนของพื้นที่โฆษณาซึ่งอยู่ในหน้า Search Result Page เช่นกัน แต่ต้องจ่ายเงินเมื่อมีการคลิ๊กเปิดเข้าไปดูเว็บไซต์ PPC มีข้อแตกต่างกับ SEO ตรงที่สามารถแสดงผลในลำดับต้น ๆ ได้ง่ายและรวดเร็ว โดยที่ไม่ต้องปรับเปลี่ยนโครงสร้างในเว็บไซต์ เพียงแค่ประมูล Keyword ที่ต้องการมา เว็บไซต์ก็สามารถแสดงอยู่ในอันดับต้น ๆ ได้ (http://seo-web.aun-thai.co.th) ในกรณีนี้ agoda.com เว็บไซต์จองที่พักโรงแรมออนไลน์เคยทำสำเร็จมาแล้ว วัตถุประสงค์ของการทำตลาดแบบดิจิทัล คือ (1) การรับรู้แบรนด์ (Brand Awareness) (2) การเพิ่มมูลค่าแบรนด์ (Brand Value) (3) สร้างชุมชนแบรนด์ (Build Brand Community) (4) การศึกษาด้านการตลาด (Education Marketing) (5) เพิ่มการเข้าชมเว็บไซต์ (Increase Website Traffic) และ (6) ให้มีลักษณะปรากฏทางออนน์ (Online Appearance) (7) สร้างโอกาสในการขาย (Generate Leads) (8) ขายออนไลน์ (Online Sale) (9) ขายแบบออฟไลน์ (Offline Sale) (10) ทำวิจัยข้อมูล (Research Data) และ (11) การดาวน์โหลดแอพพลิเคชั่น (Application Download) หลักการสำคัญของการทำการตลาดออนไลน์นั้น เนื้อหาการตลาด (Contents Marketing) มีความสำคัญมาก ต้องจัดทำเนื้อหาให้ดีและสามารถนำไปเผยได้ในหลายลักษณะได้แก่ การขียน Blog เช่น blogger.com, pantip.com รวมไปถึงการจัดทำ Online PR, บทความ, วิดีโอ, Blogs & Forums, Seeding Marketing คือการทำตลาดโดยสร้างข้อความหรือบทสนทนาให้น่าสนใจและน่าเชื่อถือตรงกับความต้องการของลูกค้า เช่น สินค้าแฟชั่น เสื้อผ้า เครื่องสำอางค์ ร้านอาหาร เครื่องใช้ในครัวเรือน เป็นต้น ความจริงความหมายของคำว่า Seeding คือการเพาะพันธ์ เพาะเมล็ดพันธุ์พืชเปรียบได้กับการปลูกเมล็ดตราสัญลักษณ์ (Branding), ส่วนอีกคำหนึ่ง คือ Influencer Marketing หมายถึงการทำการตลาดแบบอาศัยตัวบุคคล องค์กร แบรนด์ และอื่น ๆ ที่มีความน่าเชื่อถือทางสังคม เข้ามาเป็นตัวช่วยในการทำการตลาดด้วย[1]

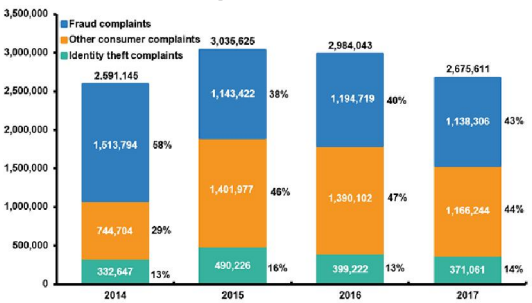
รูปภาพที่ 2
การขโมยอัตลักษณ์และการขโมยหมายเลขบัตรเครดิต
(Source: https://www.entrepreneur.com)

ส่วนเนื้อหาต่อไปนี้ เว็บไซต์วิกิพีเดีย สารานุกรมเสรี ได้แสดงให้เห็นถึงเกี่ยวกับข้อมูลส่วนบุคคลหรืออัตลักษณ์ว่า มักเป็นข้อมูลที่ไม่ได้ใช้ในการแยกแยะอัตลักษณ์ แต่หากนำมาใช้รวมกันก็อาจชี้เฉพาะตัวบุคคลได้เช่นกัน ได้แก่ ประเทศ รัฐ หรือเมืองที่มีถิ่นฐานพำนักอยู่ อายุ เพศหรือเชื้อชาติ สถานศึกษา หรือสถานที่ทำงาน ชั้นการศึกษา ผลการศึกษา เงินเดือนสินจ้าง หรือตำแหน่งหน้าที่การทำงาน ประวัติอาชญากรรม เมื่อบุคคลไม่ประสงค์ออกนาม การกล่าวถึงบุคคลนั้น มักจะประกอบด้วยข้อมูลข้างต้นสองหรือสามประการ เช่น “ผู้ชายอายุ 34 ปีที่ทำงานในห้างสรรพสินค้า X” ลักษณะเช่นนี้ เป็นการเปิดเผยข้อมูลส่วนบุคคลบางส่วน แต่ไม่ถึงกับทำให้สาธารณชนแยกแยะตัวบุคคลที่ถูกกล่าวถึงได้ว่าเป็นใคร อย่างไรก็ตามหากมีข้อมูลมากขึ้นอาจทำให้แยกแยะตัวบุคคลได้ โดยเฉพาะในคดีอาชญากรรม จึงได้มีการเสนอหลักฐานข้อมูลหลายประการที่บ่งบอกถึงตัวอาชญากร ในปี ค.ศ.1990 ได้มีการแสดงให้เห็นว่า ประชาชนชาวอเมริกัน 87 % สามารถถูกระบุเฉพาะเจาะจงได้ด้วยเพียง เพศ รหัสไปรษณีย์ และวันเกิด

(ข้อมูล : http://storylineblog.com & http://www.quizzle.com) สาเหตุหนึ่งที่ทำให้สถิติการขโมยอัตลักษณ์ในปัจจุบันมีมากขึ้น คือความโลภ หรือความต้องการทางด้านการเงินเป็นหลัก สำหรับแนวทางปฏิบัติ ที่ผู้ไม่ประสงค์ดีหรืออาชญากรนิยมใช้ในการขโมยอัตลักษณ์ 4 อย่าง ดังต่อไปนี้ คือ :

*** การละเมิดข้อมูลด้วยการขโมยระเบียนส่วนบุคคล** หมายถึง มีบุคคลกลุ่มหนึ่งพยายามฝ่าฝืนละเมิดข้อมูลด้วยการขโมยสารสนเทศที่เป็นอัตลักษณ์ส่วนบุคคลจากฐานข้อมูลขนาดใหญ่ขององค์กร อาจมีสาเหตุเกิดมาจากผู้เจาะระบบที่ต้องการอยากได้ข้อมูล หรือทำลายฐานข้อมูล หรือส่วนหนึ่งอาจจะเกิดจากความประมาท หรืออาจเกิดจากการไม่ปฏิบัติตามขั้นตอนของการรักษาความปลอดภัยที่เหมาะสม ตัวอย่างเช่น คอมพิวเตอร์แล็ปท็อปที่มีหมายเลขประกันสังคมที่ไม่ได้เข้ารหัสของทหารผ่านศึกสหรัฐ คิดเป็นจำนวนเงินถึง 26,500,000 ดอลล่าร์สหรัฐ ถูกขโมยไปจากบ้านของนักวิเคราะห์กิจการทหารผ่านศึก นักวิเคราะห์นโยบายที่ถูกละเมิดนั้นอาศัยอยู่ที่รัฐเวอร์จิเนีย และข้อมูลที่ถูกลบนั้นถูกลบออกจากสถานที่ทำงานของเขา อีกตัวอย่างหนึ่งกรณีเกี่ยวกับนักเจาะระบบ คือ เมื่อปี ค.ศ. 2010 ที่ผู้ก่อการร้ายใช้ชื่อว่า “นิรนาม” ใช้ DDoS โจมตี บริษัท มาสเตอร์การ์ด เพพาล ซิตี้แบงค์และวีซ่า โดยเจ้าของเว็บไซต์ วิกิลีกส์ (WikiLeaks) นักเจาะระบบ และผู้ก่อการร้ายทางไซเบอร์นี้ ส่วนใหญ่มองหาแนวทางที่ต้องการจะได้รับสารสนเทศที่สำคัญ โดยใช้เทคนิคการทำลายหรือทำให้ระบบการให้บริการเกิดความยุ่งเหยิง และเมื่อไม่นานมานี้ ข้อมูลผู้ใช้ในเฟซบุ๊คถูกขโมยไปกว่า 50 ล้านราย และถูกแฮกข้อมูลไปได้สำเร็จ ซึ่งก่อนหน้านี้ก็เคยถูกขโมยไปแล้วกว่า 87 ล้านรายได้รั่วไหลออกไปในปี 2559 ซึ่งข้อมูลที่หลุดรั่วออกไปนั้นได้ถูกส่งต่อไปยัง บริษัท เคมบริดจ์ อะนาลีติกา (Cambridge Analytical) บริษัทวิเคราะห์ข้อมูลในการจัดทำแคมเปญหาเสียงเลือกตั้งของประธานาธิบดี โดนัลด์ ทรัมป์ ได้นำข้อมูลไปใช้งานโดยที่ไม่ได้รับอนุญาต หรือความยินยอม จากเหตุการณ์ที่เกิดขึ้นทำให้ มาร์ก ซักเคอร์เบิร์ก (Mark Zuckerberg) CEO ของเฟซบุ๊ก ต้องเข้ารับการชี้แจงต่อวุฒิสภาสหรัฐอเมริกา เมื่อวันที่ 10–11 เมษายนที่ผ่านมา ถึงมาตรการในการดูแลข้อมูลส่วนบุคคลของผู้ใช้งาน FACEBOOK อาจจะถูกปรับสูงถึง 5 หมื่นล้านบาท (1.63 พันล้านดอลลาร์) กับกรณีการรั่วไหลของข้อมูลครั้งล่าสุด ตามระเบียบ GDPR ของสหภาพยุโรป สิ่งที่ตามมานอกจากคำถามเรื่องมาตรการความมั่นคงปลอดภัยของผู้ใช้งานก็คงหนีไม่พ้นค่าปรับที่เฟซบุ๊กอาจต้องจ่ายตามกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation หรือ GDPR) สำหรับกรณีที่เฟซบุ๊กไม่ปฏิบัติตามกฎระเบียบ จนเป็นเหตุให้มีข้อมูลผู้ใช้งานรั่วไหลออกไป ซึ่งขณะนี้คณะกรรมการคุ้มครองข้อมูลส่วนบุคคลของไอร์แลนด์ได้ประสานขอข้อมูลเพิ่มเติมจากเฟซบุ๊ก เพื่อทำการสอบสวนว่ามีข้อมูลของประชากรยุโรปได้รับผลกระทบจากเหตุการณ์ที่เกิดขึ้นอย่างไร ซึ่งหากเฟซบุ๊กถูกตัดสินว่ามีความผิดจริงอาจได้รับโทษปรับสูงถึง 5 หมื่นล้านบาท ข้อมูลส่วนบุคคลไม่ใช่เพียง ชื่อ-นามสกุล ที่อยู่ เลขบัตรประชาชน หรือเบอร์โทรศัพท์ เท่านั้น แต่รวมไปถึงข้อมูลทุกชนิดที่สามารถระบุถึงตัวบุคคลนั้น ๆ ได้ไม่ว่าทางตรงหรือทางอ้อม เช่น ข้อมูลสถานที่ตั้ง พฤติกรรมความชอบ พฤติกรรมการบริโภคสินค้าและบริการ เป็นต้น ซึ่งข้อมูลเหล่านี้มีความสำคัญเป็นอย่างยิ่งไม่เพียงแต่ความเสี่ยงที่อาจถูกฉ้อโกงทางธุรกรรมจากผู้ไม่หวังดีเท่านั้น แต่ข้อมูลทั้งหมดสามารถนำไปวิเคราะห์เพื่อผลประโยชน์การโฆษณา การเมือง การทำธุรกิจหรือการตลาดบนโลกออนไลน์ได้อย่างที่เราไม่คาดคิด

ข่าวล่าสุด ไม่นานมานี้เอง คือ เมื่อวันที่ 28 กันยายน พ.ศ. 2561 ได้มีการออกแถลงการณ์จากเฟซบุ๊ก (https://newsroom.fb.com/news/2018/09/security-update/) กรณีตรวจพบการรั่วไหลของข้อมูลผู้ใช้งานกว่า 50 ล้านรายทั่วโลก ซึ่งถูกแฮกเกอร์เจาะระบบผ่านช่องโหว่ของแพลตฟอร์มเมื่อวันที่ 25 กันยายนที่ผ่านมา ทำให้เฟซบุ๊กต้องทำการรีเซตระบบ Access Tokens ของผู้ใช้งานเพื่อป้องกันผลกระทบที่อาจเกิดขึ้น ส่งผลให้ผู้ใช้งานกว่า 90 ล้านบัญชี ถูกบังคับให้ออกจากระบบเพื่อให้เข้าสู่ระบบใหม่อีกครั้ง



รูปภาพที่ 3 การขโมยข้อมูลประจำตัว และการร้องเรียนการทุจริต (Source: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-Cybercrime)

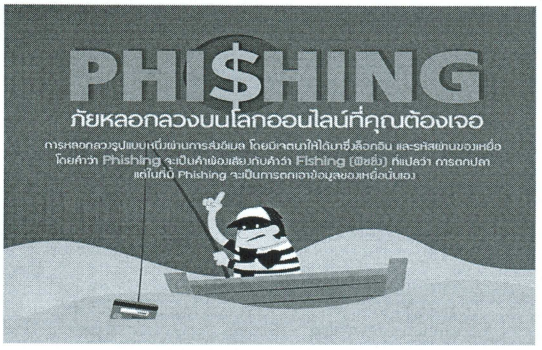
สำหรับเรื่องการขโมยข้อมูลประจำตัว และการร้องเรียนการทุจริต มีเครือข่ายผู้บริโภคและผู้ดูแลโดย Federal Trade Commission (FTC) ได้ติดตามการฉ้อโกงของผู้บริโภคและ การร้องเรียนการขโมยข้อมูลประจำตัวที่ยื่นต่อหน่วยงานบังคับใช้กฎหมายของรัฐบาลกลางรัฐและท้องถิ่นและองค์กรเอกชน พบว่า มีการขโมยข้อมูลประจำตัว 2.7 ล้านครั้ง และรายงานการฉ้อโกงที่ได้รับในปี ค.ศ.2017 มีจำนวน 1.1 ล้านคน เกี่ยวข้องกับการฉ้อโกงที่ทำให้ผู้บริโภคได้รับความเสียหาย มีมูลค่าเกือบ 905 ล้านเหรียญ ข้อมูลของผู้บริโภคที่มีความเสียหายในกรณีนี้ มีจำนวนเฉลี่ยคือ $ 429 ในประเภทการฉ้อโกงแบบการหลอกลวง มีการรายงานมากที่สุด และได้รับการจัดอันดับเป็นที่หนึ่งใน 10 ประเภทการฉ้อโกงที่ระบุโดย FTC คิดเป็นขาดทุน 328 ล้านดอลลาร์ และในปี 2560 ร้อยละ 14 ของข้อร้องเรียนทั้งหมดเกี่ยวข้องกับการขโมยข้อมูลส่วนตัว ต่อมาเรื่องข้อร้องเรียนเรื่องการขโมยข้อมูลประจำตัวเป็นครั้งที่สามที่มีการรายงานมากที่สุดต่อ FTC และเพิ่มขึ้นเกือบ 70 % จากปี 2013 ถึงปี 2015 แต่ลดลงประมาณ 24 เปอร์เซ็นต์จากปี 2015 ถึงปี 2017 การฉ้อโกงบัตรเครดิตเป็นเหตุการณ์ที่เกิดขึ้นมากที่สุด[2]

*** การจัดซื้อสารสนเทศ** ในปัจจุบันในตลาดมืดมีการซื้อขายสารสนเทศกันอย่างแพร่หลาย โดยเฉพาะสหรัฐอเมริกา มีการซื้อขายสารสนเทศกันอย่างเป็นล่ำเป็นสัน ตัวอย่างเช่น หมายเลขบัตรเครดิต ราคาสูงขึ้นเป็น $.40 ดอลล่าร์สหรัฐ, ชื่อผู้ใช้ระบบ หมายเลขรหัสลับส่วนตัวของบัญชีธนาคาร ราคา $10 ดอลล่าร์, สารสนเทศที่เป็นอัตลักษณ์รวมไปถึง วัน เดือน ปีเกิด ที่อยู่ หมายเลขเงินเดือน และหมายเลขโทรศัพท์ ราคา มีตั้งแต่ $1 ถึง $15 ดอลล่าร์สหรัฐ ในประเทศไทยก็มีข่าวเกี่ยวกับการขายข้อมูล หรือสารสนเทศลูกค้าเช่นเดียวกัน คือ มีข่าวเรื่องเฟซบุ๊กแฟนเพจ ชมรมช่วยเหลือเหยื่ออาชญากรรม ไขข้อสงสัย Call center โทรเสนอขายประกัน-สินเชื่อ มาถึงเราได้ยังไง (21 พ.ย.) เฟซบุ๊กแฟนเพจชมรมช่วยเหลือเหยื่ออาชญากรรม ได้โพสต์ภาพพร้อมข้อความระบุว่า “เปิดโปง ! ขบวนการขายข้อมูลลูกค้าธนาคารให้กับแก๊ง Call center และบริษัทขายประกัน, สินเชื่อทั่วประเทศนับล้านบัญชี ถือเป็นการละเมิดและเป็นภัยร้ายแรงต่อประเทศ โดยมีข้อความว่า

เรียนพี่น้องประชาชนและสมาชิกทุกท่าน ชมรมช่วยเหลือเหยื่ออาชญากรรม ขอเปิดเผยตัวอย่างการขายข้อมูลลูกค้าธนาคาร โดยในเอกสารฉบับนี้ประกอบไปด้วย เลขบัตรประชาชน 13 หลัก ชื่อ นามสกุลลูกค้า เบอร์โทรศัพท์มือถือและเบอร์บ้าน - สำนักงาน ที่อยู่ของลูกค้า และจำนวนเงินในบัญชีของลูกค้า ซึ่งหลายท่านอาจแปลกใจ ที่อยู่ ๆ มีใครก็ไม่รู้โทรมาหาท่านแล้วเสนอขายประกันหรือสินเชื่อบัตรเครดิตให้กับท่าน รวมทั้งแก๊ง Call center ที่โทรหาท่าน โดยที่ท่านก็ไม่รู้ว่าพวกนี้ไปเอาเบอร์ท่านมาจากไหน และพวกนี้ทราบข้อมูลของท่านทุกอย่าง ทำให้บางรายตกเป็นเหยื่อของแก๊ง Call center สูญเงินเก็บทั้งชีวิต โดยเฉพาะกลุ่มผู้สูงอายุที่มีเงินเก็บจำนวนมาก ข้อมูลเหล่านี้ถูกซื้อขายกัน ในราคาตั้งแต่ 3 บาท ไปจนถึง 50 บาท ต่อ 1 รายชื่อพร้อมข้อมูลทุกอย่างตามที่กล่าวไว้ข้างต้น[3]

*** การหลอกลวงทางอินเทอร์เน็ต (Phishing)** ฟิชชิง คือ เป็นการใช้อีเมลลตลบตะแลง โดยพยายามให้ผู้รับทำการเปิดเผยข้อมูลส่วนบุคคลออกมา เช่น รหัสผ่านหรือหมายเลขบัตรเครดิต, ชื่อและชื่อผู้ใช้ที่อยู่และหมายเลขโทรศัพท์, รหัสผ่านหรือ PIN, หมายเลขบัญชีธนาคาร, บัตรเดบิต/บัตรเอทีเอ็ม, รหัสการตรวจสอบความถูกต้องของการ์ด (CVC) หรือค่าการตรวจสอบการ์ด (CVV) หมายเลขประกันสังคม (SSN) เป็นต้น ซึ่งเป็นเสมือนการใช้เหยื่อเกี่ยวเบ็ดเพื่อล่อปลาให้มาติดเบ็ดหรือการปลอมแปลงอีเมลจากเหล่าแฮกเกอร์ โดยจะทำให้เหมือนว่าถูกส่งมาจากจากเว็บไซต์ที่ทำธุรกรรมด้านค้าขายทางอินเทอร์เน็ต เว็บไซต์ทำการประมูลซื้อขายทางออนไลน์ ธนาคาร และแหล่งสินเชื่อบัตรเครดิต เช่น Citibank eBay และ PayPal ลักษณะการหลอกหลวงได้แก่ ส่งอีเมลไปตามเหล่าสมาชิกหรือลูกค้าเหล่านั้น รวมถึงการส่งข้อความมาทาง Messenger เป็นลิงค์ให้เข้าไปยังเว็บหลอกที่ถูกสร้างขึ้นมาเหมือนกับเว็บของจริงเพื่อให้เหยื่อกรอกข้อมูลส่วนตัว เช่น User Name, Password หมายเลขบัตรเครดิตต่าง ๆ ที่นี้เมื่อเหยื่อกรอกข้อมูลลงไปแล้วพวกแฮกเกอร์ก็จะนำข้อมูลเหล่านั้นไปใช้หาผลประโยชน์ในทางที่ผิด ทำให้ความเสียหายตกอยู่กับเจ้าของข้อมูลเหล่านั้น ซึ่งพฤติกรรมเหล่านี้ก็คล้ายกับการอ่อยเหยื่อตกปลา โดยหวังให้ปลามาฮุบเหยื่อไปกินนั่นเอง[4] หรืออีกความหมายหนึ่งตามทรรศนะของ Nattapon Rakthong ได้กล่าวว่า Phishing แผลงมาจากคำว่า fishing แปลว่าการตกปลา ซึ่งมีความหมายถึง การปล่อยให้ปลามากินเหยื่อที่ล่อไว้ ตัวอย่าง ของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่

น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบ และใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น มักจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง



รูปภาพที่ 4 แสดงการหลอกลวงทางอินเทอร์เน็ต (Fishing) การตกปลา โดยความหมาย คือ การตกเอาข้อมูลของเหยื่อนั่นเอง (https://www.uih.co.th/th/knowledge/phishing)

การหลอกลวงฟิชชิงนั้นเป็นเรื่องยากสำหรับคนทั่วไปเพราะ (1) การปลอมเว็บไซต์ที่เหมือนกันมากแทบแยกไม่ออก (2) แค่เป็น https:// ไม่ใช่ว่าปลอดภัยทุกเว็บ เพราะสมัยนี้ใคร ๆ ก็ทำ https ได้ (3) อื่น ๆ วิธีการที่คุณจะตรวจสอบว่าเว็บที่คุณกำลังจะกรอกข้อมูลที่สำคัญหรือจะทำธุรกรรมต่าง ๆ เป็นการหลอกลวงแบบฟิชชิงนั้นต้องดูจากหลาย ๆ อย่างดังนี้ (1) ความเป็นเหตุเป็นผล เช่น ผมไม่เคยโหลดแอพที่เรียกเก็บเงินผมในอีเมล์เลย ผมจะโดนเก็บเงินได้ไง หรือบางคนไม่ได้ใช้ Apple เลย จะมาเรียกเก็บเงินได้ไง อะไรประมาณนี้ครับ (2) ตรวจสอบข้อมูลทางเทคนิคเบื้องต้น เช่น โดเมนส่วนใหญ่ก็จะเป็นชื่อเดียวกันกับบริษัทหรือแบรนด์ เช่น Apple ก็ควรมีโดเมนเป็น www.apple.com และวิธีการดูโดเมนหลัก สมมุติว่าคุณเจอโดเมน www.xxxx.yyyy.zzzz.com ให้คุณตัดที่เครื่องหมายจุด . ที่ 2 โดยนับจากด้ายขวามือของคุณก็จะได้เป็น zzzz.com อย่างกรณีที่ผมเจอ https://cppleid.cpple.com.th-acces.me ก็จะได้โดเมนจริงเป็น th-acces.me ซึ่งมันไม่ได้เกี่ยวอะไรกับ Apple เลย (3) ลองเอาโดเมนที่ได้ไปตรวจสอบว่าใครเป็นเจ้าของในเว็บ ด้วยเว็บ https://www.godaddy.com/whois โดยกรอกโดเมนหลักไปแล้วก็กด Search[5]

ด้วยอินเทอร์เน็ตทำให้ชีวิตประจำวันของคนเราสะดวกสบายมากขึ้น การติดต่อสื่อสารกับเพื่อนฝูง ญาติพี่น้อง หรือแม้แต่คนไม่รู้จัก ก็สามารถติดต่อสื่อสารกันได้อย่างรวดเร็ว โดยเฉพาะโลกโซเชียลมีเดีย อาทิ เฟซบุ๊ก แอพพลิเคชั่นไลน์ ฯ ลฯ แต่ความสะดวกสบายนี้มีอันตรายแฝงมาด้วย เพราะกลับกลายเป็นเครื่องมือที่ช่วยทำให้มิจฉาชีพเป็น “โจรออนไลน์” หรือ “โจรไซเบอร์” ที่แม้จะอยู่ไกลจากเหยื่อก็สามารถเข้ามาใกล้ชิด แล้วตีสนิทตุ๋นเงินไปได้โดยง่ายหากไม่ระมัดระวัง ซึ่งปัจจุบันมีข่าวเกี่ยวกับการ “ฉ้อโกง” แทบไม่เว้นแต่ละวัน จนมีสถิติการกระทำผิดและถูกหลอกลวงทางออนไลน์เพิ่มสูงขึ้นทุกปี ส่วนที่ไม่เป็นข่าวก็มีอีกจำนวนไม่น้อย

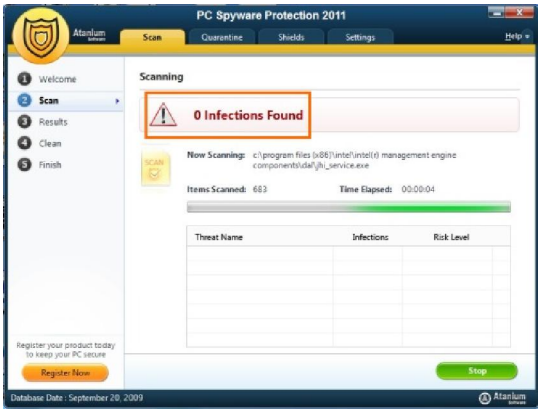
เกี่ยวกับกรณีดังกล่าวกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) อธิบายภาพรวมของภัยคุกคามทางไซเบอร์ในยุคปัจจุบันว่า จากข้อมูลสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) หรือ สอธพ. พบว่า สถิติ “ภัยคุกคามไซเบอร์” เติบโตขึ้นอย่างรวดเร็ว จากปี 2554 ที่มีผู้เข้าแจ้งความแค่หลักร้อย แล้วเพิ่มเป็นหลักพันตั้งแต่ปี 2556 และในช่วง 2 เดือนแรกของปี 2560 มีจำนวนถึง 842 กรณี เมื่อเทียบช่วงเดียวกันของปี 2559 ที่มี 713 กรณี ซึ่งการเข้าถึงและเล่นโซเชียลมีเดียของครัวเรือนที่เพิ่มขึ้น ส่งผลให้เกิดภัยคุกคามไซเบอร์เพิ่มตามมาด้วย ไม่ว่าจะเป็นการโจมตีด้วยไวรัสโปรแกรม (malicious code) โดยเมื่อสิ้นปี 2559 มีผู้เข้าแจ้งความแล้วถึง 1,020 กรณี คิดสัดส่วน 26.86 % เทียบจากช่วงก่อนปี 2556 ที่มีไม่ถึงหลักร้อยกรณี และเป็นตัวเลขเดียวกับภัยของการเจาะเข้าใช้ระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต (Intrusion) ส่วนความผิดที่เกี่ยวกับการหลอกลวงซื้อขายทางออนไลน์ (Fraud) มีสถิติสูงรองลงมา ในสัดส่วนใกล้เคียงคือ 26.39 %

การจับกุมของตำรวจ หรือการแจ้งความที่ถูกต้มตุ๋นหลอกเอาทรัพย์สินในห้วง 3 ปีที่ผ่านมาจนถึงปัจจุบัน ช่องทางโซเชียลมีเดียที่คนร้ายนิยมใช้มากที่สุดคือ เฟซบุ๊ก! ไม่ว่าจะเป็นการปลอมเฟซบุ๊กแชทหาเพื่อนหลอกยืมเงิน ขายสินค้าหางาน แชร์ออนไลน์ ประมูลทองคำ บริจาคช่วยเหลือต่าง ๆ ฯลฯ ซึ่งล่าสุดเมื่อวันที่ 11 เมษายน ที่ผ่านมา ตำรวจกองปราบปราม ได้จับกุม น.ส.ปาวีณา สุขฉิม อายุ 33 ปี สืบเนื่องจากเมื่อช่วงกลางปี 2560 น.ส.ปาวีณาได้ปลอมเฟซบุ๊กของ “แอม” เสาวลักษณ์ ลีละบุตร ศิลปินนักร้องชื่อดัง ก่อนโพสต์ข้อความชวนเชื่อว่า สามารถจัดหาสถานที่ทำงานหรือพาไปทำงานยังต่างประเทศได้ ซึ่งผู้ที่สนใจจะได้รับเงินเดือนประมาณ 8 หมื่นบาท

แต่จะต้องยอมจ่ายเงินเป็นค่าดำเนินการตั้งแต่หลักหมื่นไปจนถึงหลักแสนบาท ตามแต่ความยากง่ายของแต่ละประเทศที่ผู้เสียหายต้องการไปทำงาน ซึ่งมีเหยื่อหลงเชื่อจำนวนมาก สร้างความเสียหายกว่า 10 ล้านบาท นอกจากนี้ยังมีการตุ๋นเหยื่อของ “แก๊งโรแมนซ์สแกม” หรือ “แก๊งแสร้งรักออนไลน์” ที่มีคนไทยและชาวผิวสีร่วมขบวนการ ที่ผ่านมาตำรวจจับกุมไปแล้วหลายแก๊ง แถลงข่าวประชาสัมพันธ์เตือนภัยไปแล้วก็หลายหน แต่ก็ยังมีก่อเหตุอยู่เนือง ๆ เช่นกัน โดยล่าสุดวันที่ 22 เมษายน ที่ผ่านมา ก็มีการแถลงผลจับกุมชาวไนจีเรียร่วมก๊วนคนไทย ส่วนพฤติการณ์เดิม ๆ คือ แบ่งหน้าที่กันหลอกผู้เสียหายทั้งชาวไทยและชาวต่างชาติ ลักษณะใช้รูปโปรไฟล์หน้าตาดีหลอกคุยกับผู้เสียหายผ่านทางโซเชียลมีเดีย โดยเฉพาะเฟซบุ๊ก แล้วอ้างว่ามีสินค้าที่จะส่งเป็นของขวัญให้ผู้เสียหาย แต่ติดขั้นตอนศุลกากร จนออกอุบายให้ผู้เสียหายโอนเงินมาช่วยเหลือเพื่อนำสินค้าออกไป เมื่อผู้เสียหายหลงเชื่อโอนเงินมาก็จะปิดเฟซบุ๊กหนีทันที[6]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ได้มีการบันทึกสถิติล่าสุดเกี่ยวกับการทำความผิดออนไลน์เฉพาะของปี 2561 ตั้งแต่เดือนมกราคม-มีนาคม ดังนี้ การฉ้อฉลหลอกลวงเพื่อผลประโยชน์ (Fraud) เกิดขึ้นแล้วจำนวน 235 ครั้ง เทียบกับทั้งปี 2560 ที่เกิดขึ้นจำนวน 841 ครั้ง, การพยายามบุกรุกเข้าระบบ (Intrusion Attempts) เกิดขึ้นแล้วจำนวน 233 ครั้ง เทียบกับทั้งปี 2560 ที่เกิดขึ้นจำนวน 939 ครั้ง, การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions) เกิดขึ้นแล้วจำนวน 132 ครั้ง เทียบกับทั้งปี 2560 ที่เกิดขึ้นจำนวน 570 ครั้ง, โปรแกรมไม่พึงประสงค์ (Malicious Code) เกิดขึ้นแล้วจำนวน 33 ครั้ง เทียบกับทั้งปี 2560 ที่เกิดขึ้นจำนวน 271 ครั้ง และการเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต (Information Security) เกิดขึ้นแล้วจำนวน 3 ครั้ง เทียบกับทั้งปี 2560 ที่เกิดขึ้นจำนวน 68 ครั้ง ทำให้เห็นว่าแนวโน้มของการหลอกลวงเพื่อผลประโยชน์นั้นยังจะทะยานขึ้นไปอีก ซึ่งขณะนี้จากสถิติการหลอกลวงซื้อขายออนไลน์ เป็นภัยออนไลน์ที่พบมากเป็นอันดับ 2 จากภัยคุกคามออนไลน์ทั้งหมด

*** การติดตั้งโปรแกรมการสอดแนมหรือจารกรรม** หมายถึง การกระทำโดยผิดกฎหมายโดยใช้โปรแกรมคอมพิวเตอร์ที่เรียกว่า สปายแวร์ (Spyware) เพื่อให้ได้ความลับในการแลกเปลี่ยนสินค้าจากคู่แข่งขัน เป็นลักษณะการสอดแนมหรือขโมยความลับทางการค้าไปให้กับคู่แข่งขันทางธุรกิจ การสอดแนมหรือจารกรรม เกิดจากผู้ใช้งานคอมพิวเตอร์หลงเล่ห์เหลี่ยม โดยการดาวน์โหลดซอฟต์แวร์มาใช้ และโปรแกรมสปายแวร์จะทำการติดตั้งลงในระบบทันที เมื่อซอฟต์แวร์ถูกติดตั้งเรียบร้อยแล้ว ซอฟต์แวร์ก็จะทำหน้าที่รับการเคาะจากแป้นพิมพ์เข้าสู่ระบบ และสามารถดึงเอาข้อมูลที่เป็นอัตลักษณ์ของบุคคลออกมา เช่น ชื่อบัญชีผู้ใช้ รหัสผ่าน หมายเลขบัตรเครดิต หรือสารสนเทศอื่น ๆ ที่อ่อนไหว ในบางครั้งสปายแวร์อาจแอบซ่อนตัวมากับโฆษณาสินค้าเล็ก ๆ (Popup) ที่ขึ้นมาตามเว็บไซต์ต่าง ๆ ที่เราได้เข้าไปเยี่ยมชม โดยที่เราซึ่งเป็นผู้ใช้ไม่รู้ตัวมาก่อน ส่วนใหญ่จะเป็นโฆษณาขายของหรือชวนทำธุรกิจขายตรง บางทีก็เป็นภาพลามกอนาจาร ชวนให้คลิกเป็นต้น[7] เมื่อ Spyware เข้ามาในเครื่องของเราได้แล้วซึ่งจะส่งผลดังนี้ คือ (1) คอมพิวเตอร์ทำงานช้าลง หรือแฮงก์บ่อยกว่าปกติ เนื่องจาก Spyware จะทำการเปิดใช้โปรแกรมบางอย่างโดยที่ผู้ใช้ไม่รู้ตัว (2) ทำให้การรับส่งข้อมูลผ่านอินเทอร์เน็ตช้าลง (3) ทำให้การเชื่อมต่ออินเทอร์เน็ตหลุดบ่อย มีผลทำให้ค่าโทรศัพท์สูงผิดปกติอาการของเครื่องที่ติด Spyware การสังเกตว่าเครื่องคอมพิวเตอร์ของเราหลงติดตั้งสปายแวร์หรือไม่ ให้สังเกตได้ง่าย ๆ ดังนี้ (1) มีโฆษณาเล็ก ๆ หรือ popup กระโดดขึ้นมาตลอดเวลาทั้งที่ไม่ได้เชื่อมต่ออินเทอร์เน็ต (2) หน้าแรกของโฮมเพจเปลี่ยนไปโดยที่เราไม่ได้ปรับเปลี่ยนหรือแก้ไข (3) เมื่อเข้าสู่เว็บไซต์ใดเว็บไซต์หนึ่งแล้วเข้าไม่ได้ บราวเซอร์กลับไปเปิดเว็บอีกเว็บหนึ่งแทน (4) สังเกตว่าจะมีแถบเครื่องมือใหม่ ๆ ที่ไม่เคยเห็นหรือไม่คุ้นเคยปรากฏขึ้นบนเว็บบราวเซอร์ (5) บริเวณ System Tray มีโปรแกรม หรือไอคอน แปลก ๆ แสดงอยู่ (6) เมื่อเรียก Search Engine แทนที่ผลการค้นหาที่ได้จะเป็นผลการค้นหาจาก Search Engine บราวเซอร์กลับไปเปิดเว็บอีกเว็บหนึ่งแทน (7) ฟังก์ชันบนคีย์บอร์ดที่เคยทำงานได้ปกติกลับทำงานไม่ได้ เช่น กด Tab แล้วใช้งานไม่ได้ (8) ข้อความแสดงความผิดพลาดของ Windows แสดงบ่อยจนผิดปกติ และ (9) เครื่องทำงานช้าลงอย่างเห็นได้ชัด



รูปภาพที่ 5 ตัวอย่างโปรแกรมตรวจสอบและป้องกัน Spyware (https://notebookspec.com)

ปัจจุบันได้มีการได้มีการออกกฎหมายเรื่องจารกรรมทางเศรษฐกิจในปี ค.ศ. 1996 เพื่อป้องกันการสอดแนมความลับในการแลกเปลี่ยนสินค้า ในขณะเดียวกันก็มีบางคนบางกลุ่มได้ใช้ความฉลาดเกี่ยวกับการให้ได้ข้อมูลความลับเกี่ยวกับการแข่งขัน โดยการใช้ความสามารถพิเศษอย่างถูกกฎหมาย หรือการอาศัยช่องโหว่ทางกฎหมายมาช่วยเพื่อให้ได้ข้อมูลความลับเหล่านั้น เช่น ความพยายามเก็บรวบรวมสารสนเทศที่มีความไม่เหมาะสมนำไปเผยแพร่ในที่สาธารณะ[8] ในอีกกรณีหนึ่ง ปัจจุบันนี้มีเด็กหรือเยาวชน รวมถึงผู้ใช้งานทั่วไปใช้เวลาไปกับสมาร์ทโฟนมากขึ้นเป็นลำดับ ไม่ว่าจะเป็นการใช้บนสื่อสังคมออนไลน์ หรือกิจกรรมอื่น ๆ ทำให้มีความเสี่ยงของการถูกกลั่นแกล้งไซเบอร์, sexting, และการโจรกรรม โดยเฉพาะจะมีการการติดตั้งโปรแกรม SpyToApp[9] เป็นการสอดแนมโทรศัพท์มือถือ และโทรศัพท์มือถือติดตามเสนอซอฟต์แวร์ขั้นสูงเฝ้าระวัง และติดตามเทคโนโลยีหุ่นยนต์ SpyToApp เป็นโปรแกรมติดตามโทรศัพท์มือถือที่ดีที่สุดเพื่อตรวจสอบข้อ, โทรศัพท์, ตำแหน่ง GPS, ติดตาม whatsapp, facebook, ข้อความที่ viber และ yahoo. เป็นนักสืบเอกชนดิจิตอลของคุณส่วนบุคคล, ให้คุณได้ตลอดเวลา, ได้เข้าถึงข้อมูลที่เก็บรวบรวมจากสมาร์ทโฟน หรืออุปกรณ์มือถือที่คุณเลือก

จากข้อมูลข้างต้นจะเห็นได้ว่า การขโมยอัตลักษณ์ได้กลายมาเป็นภัยคุกคามบนโลกไซเบอร์ที่ทุกคนต้องเฝ้าระวังอย่างมาก กรุงเทพธุรกิจออนไลน์ ได้ลงข่าวสถิติและงานวิจัยเรื่อง “สเตท ออฟ เดอะ อินเทอร์เน็ต” ของ “คอนซูเมอร์ รีพอร์ส” กลุ่มเฝ้าระวังของสหรัฐพบว่า เมื่อปีที่ผ่านมาการขโมยอัตลักษณ์ได้เพิ่มขึ้นอย่างรวดเร็ว และที่น่าตกใจคือ ข้อมูลจำนวนมหาศาลในเฟซบุ๊คที่ได้จากสมาชิกเกือบ 900 ล้านคน และความเต็มใจของเหล่าสาวกที่แชร์ข้อมูลที่เป็นส่วนตัวมาก ๆ กลายเป็นประโยชน์ของเหล่านายจ้าง บริษัทประกัน ทนายความที่จัดหาเรื่องหย่า รวมถึงโจรขโมยอัตลักษณ์ และอาชญากรรมประเภทอื่น ๆ ให้พิจารณาดูข้อมูลต่อไปนี้ คือ ผู้ใช้ 4.7 ล้านคนกด “ไลท์” หน้าเฟซบุ๊คเกี่ยวกับความเจ็บป่วยและการรักษาของพวกเขา (รายละเอียดที่บริษัทประกันอาจใช้ในการปฏิเสธการรับประกัน หรือจ่ายค่าสินไหมทดแทนได้), ผู้ใช้ 4.8 ล้านคน ใช้เฟซบุ๊คเพื่อบอกสถานที่ และเวลากำลังจะไป (บอกใบ้ให้ขโมยรู้), ผู้ใช้ 20.4 ล้านคนโพสต์วันเกิด ซึ่งโจรขโมยอัตลักษณ์ชอบ, ผู้ใช้ 39.3 ล้านคน ระบุสมาชิกในครอบครัวไว้ในโปรไฟล์ของตนเอง, ผู้ใช้ 900,000 คนถกกันเรื่องเงิน ๆ ทองๆ บนหน้าวอลล์, ผู้ใช้ 1.6 ล้านคน กด “ไลท์” หน้าเพจองค์กร/หน่วยงานทางด้านชาติพันธุ์หรือเชื้อชาติ, ผู้ใช้ 2.3 ล้านคน กด “ไลท์” หน้าเพจเกี่ยวกับเรื่องเพศ, ผู้ใช้ 7.7 ล้านคน กด “ไลท์” หน้าเพจขององค์กร/หน่วยงานทางด้านศาสนา, ผู้ใช้ 2.6 ล้านคน แลกเปลี่ยนความคิดเห็นเรื่องแอลกอฮอล์เพื่อสันทนาการบนหน้าวอลล์ของตัวเอง, ผู้ใช้ 4.6 ล้านคนคุยกันเรื่องชีวิตรักของตัวเองบนหน้าวอลล์ รายงานชิ้นนี้ได้สัมภาษณ์ผู้ที่เกี่ยวข้องกว่า 24 คน ประกอบด้วยผู้เชี่ยวชาญด้านความปลอดภัย ทนายเรื่องความเป็นส่วนตัว นักพัฒนาแอพพลิเคชั่นและเหยื่อที่ถูกละเมิดความเป็นส่วนตัวและความปลอดภัย และได้สำรวจครอบครัวที่ออนไลน์ 2,002 ครอบครัว โดย 1,340 ครอบครัวเล่นเฟซบุ๊ค พบว่าปัญหาหลักเกิดมาจาก (1) การไม่ได้ใช้เครื่องมือควบคุมความเป็นส่วนตัว 13 ล้านคนบอกว่าไม่ได้ตั้งค่า หรือไม่รู้เกี่ยวกับเครื่องมือและ 28 % แชร์ข้อมูลทั้งหมด และให้คนอื่นดู แม้ไม่ใช่เพื่อน (2) เฟซบุ๊คทำการเก็บข้อมูลมากกว่าจินตนาการ (3) ข้อมูลของผู้ใช้ถูกแชร์ออกไปอย่างกว้างขวาง (4) การป้องกันทางกฎหมายยังไม่ได้มาตรฐาน (5) ครอบครัวที่เล่นเฟซบุ๊ค 11 % บอกว่า เจอปัญหานี้มาตั้งแต่ปีที่แล้ว ตั้งแต่มีคนแอบใช้ล็อกอินโดยไม่ได้รับอนุญาต ไปจนถึงการก่อกวน หรือข่มขู่ โดยคิดเป็นจำนวนราว 7 ล้านครอบครัว ซึ่งมากกว่าปีที่แล้ว 30 % ส่วนแนวทางในการป้องกัน คือ (1) ไม่ควรเปิดเผยชื่อผู้ใช้ และ ID ให้ผู้อื่นรู้ (2) ตั้งค่าความเป็นส่วนตัว (3) ไม่ควรเปิดเผยข้อมูลอัตลักษณ์ (4) ไม่ควรแชร์ในเรื่องสารสนเทศที่มีความอ่อนไหว เช่น ข้อมูลการรักษาสุขภาพ (5) ติดตั้งซอฟต์แวร์รักษาความปลอดภัย

และสแกนไวรัส (6) ใช้คอมพิวเตอร์อย่างมีวิจารณญาน ไม่หลงเชื่อคนอื่นง่าย (7) เรียนรู้ให้เท่าทันเทคโนโลยี และวิธีป้องกันความปลอดภัยที่ดี

สำหรับวิธีป้องกันโดนหลอกลวงทางออนไลน์หรือทางอินเทอร์เน็ต คือ (1) กรณีซื้อสินค้าออนไลน์ ควรตรวจสอบประวัติของเพจ, ชื่อเจ้าของบัญชีที่จะโอนเงิน, วิดีโอคอลพูดคุยกับร้านค้า เพื่อเซฟหน้าจอหรือเซฟวิดีโอคอลที่คุยกัน ถ้าร้านค้าไม่ส่งสินค้ามาวิดีโอคอลจะเป็นหลักฐานสำคัญในการดำเนินคดีต่อไป (2)การรับสมัครงานออนไลน์ที่พบเห็นในโลกอินเทอร์เน็ต มักมีคนร้ายแฝงตัวเข้ามาหลอกให้ประชาชนส่งสำเนาบัตรประชาชน, สมุดบัญชีธนาคาร, บัตรเอทีเอ็ม เพื่อไปใช้กระทำความผิด คนที่คิดจะทำงานออนไลน์ควรไปสมัครที่ทำงานที่อ้างถึง เพื่อตรวจสอบว่าบริษัทหรือร้านค้าดังกล่าวมีตัวตนหรือไม่ และ (3) เก็บหลักฐานการพูดคุย, หลักฐานการโอนเงินทุกครั้งที่คิดจะซื้อของทางออนไลน์ หรือการทำธุรกรรมอื่น ๆ ที่กลุ่มมิจฉาชีพหากลวิธีมาหลอกลวงเอาทรัพย์สินเงินทอง

การป้องกันการขโมยอัตลักษณ์ สามารถป้องกันได้หลายแนวทาง หากใช้อีเมลควรจะมีโปรแกรมกลั่นกรองอีเมล์ (Filter) ซึ่งจะมีการเตือนเกี่ยวกับความไม่น่าไว้ใจทางอีเมล รวมถึงควรมีการติดตั้งโปรแกรมแอนตี้ไวรัส การเข้าใช้เว็บไซต์ต้องเข้าใช้เว็บไซต์ที่ไว้ใจได้ เพราะเว็บไซต์ที่หลอกลวงทางอินเทอร์เน็ตเช่นกัน และเล่ห์อุบายทางโทรศัพท์ หรือการหลอกลวงผ่าน Call Center ก็ต้องระมัดระวังเช่นกันไม่เชื่อคนง่าย แม้กระทั่งการถ่ายสำเนาเอกสาร ก็ต้องระมัดระวังด้วยเช่นกัน คนเป็นจำนวนมากไม่ระมัดระวังเกี่ยวกับการถ่ายภาพอัดสำเนาซึ่งปัจจุบันมันมีความความเสี่ยงจากการขโมยอัตลักษณ์มากที่เป็นเช่นนี้ เพราะว่าร้านที่รับถ่ายภาพอัดสำเนาปัจจุบัน มีการถ่ายอัดสำเนาบรรจุลงไปที่ฮาร์ดไดร์ฟ โดยเฉพาะการทำงานของคอมพิวเตอร์, เอกสารที่ถูกวาดภาพหรือสแกนจะถูกจัดเก็บไว้ที่ฮาร์ดไดร์ฟ หลังจากนั้นก็จะถูกพิมพ์ออกมาโดยเครื่องมือในการคัดลอก ดังนั้น อย่างน้อยเครื่องมือในการคัดลอกควรจะมีการปรับแต่งโดยเฉพาะ แล้วให้ฮาร์ดไดร์ฟเขียนทับในการทำลายข้อมูล หรือใช้การเข้ารหัสลับ, สำเนาใบคืนภาษีของคุณอาจจะหลบซ่อนอยู่บนการสำเนาสาธารณะที่ห้องสมุดท้องถิ่นของคุณ หรือสำเนาการซื้อของที่คุณใช้ก่อนที่จะส่งจดหมายกลับไปยังการบริการรายได้ภายในของคุณ ผู้เจาะระบบที่ฉลาดจะเรียกความมั่งคั่งของศักยภาพสารสนเทศออกมาจากร้านถ่ายสำเนาสาธารณะร้านใดร้านหนึ่งก็ได้ ส่วนการป้องกัน Spyware นั้น สามารถทำได้ด้วยวิธีต่อไปนี้ คือ (1) ไม่คลิกบนหน้าต่างเล็ก ๆ หรือ popup ที่ปรากฏขึ้นมาอัตโนมัติ (2) ควรเลือกคำตอบ “No” ทุกครั้งที่มีคำถามต่าง ๆ ที่มาจาก popup หรือเป็นคำถามที่เราไม่เข้าใจ หรือหากมีปุ่มกดปิดหน้าต่างได้ ก็ควรกดปุ่มปิด (3) ระวังในการดาวน์โหลดซอฟต์แวร์ที่จัดให้ดาวน์โหลดฟรี ไม่ใครดาวน์โหลดจากเว็บไซต์ที่ไม่น่าเชื่อถือ และ (4) ไม่ควรตามอีเมล์ลิงค์ที่ให้ข้อมูลว่ามีการเสนอซอฟต์แวร์ป้องกัน Spyware และ (5) ติดตั้งโปรแกรมป้องกันสปายแวร์ (Spyware)

ดังนั้น จะเห็นได้ว่า วิธีการการขโมยอัตลักษณ์ในปัจจุบัน มีหลายรูปแบบมาก ยิ่งมีจำนวนผู้ใช้คอมพิวเตอร์และโซเชียลมีเดียมากขึ้นเท่าใด โอกาสเสี่ยงในการถูกขโมยอัตลักษณ์ยิ่งมีมากขึ้นเท่านั้น เพราะว่าในจำนวนผู้ใช้เหล่านั้นมีทั้งผู้ประสงค์ดี และไม่ประสงค์ดีมีอยู่ปะปนกันไป ส่วนเป้าประสงค์ที่ทำให้เกิดภัยคุกคามในโลกไซเบอร์ทวีจำนวนมากขึ้นนั้น ส่วนหนึ่งเกิดมาจากการแสวงหาเงินและกำไรบนโลกอินเทอร์เน็ตนั่นเอง.

บรรณานุกรม

1. Praewpilai Chinsakchai, (2017), “Social Media Literacy: Connecting to ASEAN & Global Professional” สไลด์การบรรยาย, มหาวิทยาลัยศรีปทุม, 29 มิถุนายน พ.ศ. 2560.
2. Federal Trade Commission, Consumer Sentinel Network, Facts + Statistics: Identity theft and cybercrime, (Cite 2019, February 22) Available from https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
3. เฟซบุ๊ก ชมรมช่วยเหลือเหยื่ออาชญากรรม, เปิดโปง! ขบวนการขายข้อมูลลูกค้าธนาคาร ให้แก๊ง Call center, (Cite 2019, February 10) Available from https://www.sanook.com/news/2105606/

4. Web Master, รู้เท่าทัน พร้อมป้องกัน การถูกขโมยข้อมูลส่วนตัวบนโซเชียลมีเดียชื่อดัง, (Cite 2019, February 10) Available from https://www.etda.or.th/content/how-to-protect-your-private-facebook-data.html
5. Nattapon Rakthong, ฟิชชิง การหลอกลวงที่ยังไม่หายไปจากโลกอินเทอร์เน็ต, (Cite 2019, February 10) Available from https://medium.com/@nattaponra
6. ทีมข่าวอาชญากรรม, "ภัยไซเบอร์"ยอดพุ่ง!! เฟซบุ๊กแชมป์ เหยื่อเสียท่าเพราะความอยาก : คอลัมน์... เจาะประเด็นร้อน" (Cite 2019, February 17) Available from http://www.komchadluek.net/news/scoop/322782
7. peanutt199, การสอดแนมข้อมูลคอมพิวเตอร์โดยสปายแวร์, (Cite 2019, February 17) Available from https://sites.google.com/site/peanutt199/002
8. สุพล พรหมมาพันธุ์, (2014). การขโมยอัตลักษณ์: ภัยคุกคามใกล้ตัว, CIO World & Business, ISSUE144, May 2014.
9. สาวจิ๋นนี่, วิธีการสอดแนมในโทรศัพท์มือถือฟรีโดยไม่ต้องสัมผัสโทรศัพท์เป้าหมาย ?,, (Cite 2019, February 17) Available from http://blog.spytoapp.com/th/how-to-spy-on-mobile-phone-free-without-touching-the-targets-phone/