การวิเคราะห์รูปแบบการโจรกรรมอัตลักษณ์บุคคลบนโลกไซเบอร์

An Analysis of Structural Form of Identity Theft in Cyber

กิตติยา แก้วมี

Kittiya Kaewmee

หลักสูตรศิลปศาสตรดุษฎีบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม จุฬาลงกรณ์มหาวิทยาลัย

E-mail: kittiya.psed8@gmail.com

Received: June 22, 2020

Revised: July 14, 2020

Accepted: July 17, 2020

บทคัดย่อ

บทความนี้มีวัตถุประสงค์ในการนำเสนอการโจรกรรมอัตลักษณ์บุคคลบนโลกไซเบอร์ โดยมีเนื้อหาเกี่ยวกับรูปแบบการโจรกรรม ลักษณะข้อมูล ประเภทของการโจรกรรม ตลอดจนแนวทางการแก้ไขปัญหา เนื่องจากโลกยุคปัจจุบันเป็นโลกของเทคโนโลยีสารสนเทศและการสื่อสารอย่างไร้พรมแดนที่เชื่อมโยงโลกเข้าด้วยกันของอินเทอร์เน็ต เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทต่อการดำเนินชีวิตประจำวันเป็นอย่างมาก จนเรียกได้ว่าเป็นส่วนหนึ่งของการดำรงชีวิต เพราะการใช้อินเทอร์เน็ตช่วยอำนวยความสะดวกและตอบสนองความต้องการของมนุษย์ในการใช้งาน เพื่อการแลกเปลี่ยนข้อมูลระหว่างกัน ซึ่งข้อมูลต่าง ๆ จะถูกส่งจากคอมพิวเตอร์ของเราไปสู่ระบบอื่น ๆ ที่เป็นตัวรองรับในการจัดการเพื่อให้ได้มาซึ่งสิ่งที่ต้องการ ทำให้ทุกคนมักจะเชื่อใจและไว้วางใจในการเปิดเผยข้อมูลส่วนบุคคลออกสู่สาธารณะ จึงเป็นช่องโหว่ให้อาชญากรสามารถเข้าถึงข้อมูลสำคัญและเป็นความลับของบุคคลได้ ไม่ว่าจะเป็นข้อมูลบัญชีธนาคาร ข้อมูลเครดิต การเสียภาษี เพื่อนำข้อมูลไปสร้างเป็นบัญชีปลอมในการทำธุรกรรมต่าง ๆ เช่น การทำใบขับขี่ สูติบัตร หนังสือเดินทาง หรือแม้แต่การกระทำผิดภายใต้ชื่อของเหยื่อผ่านการใช้ยุทธวิธีต่าง ๆ โดยการนำเทคโนโลยีที่ทันสมัยมาใช้เพื่อเป็นส่วนหนึ่งของเครื่องมือในการประกอบอาชญากรรม เพื่อหลีกเลี่ยงการถูกลงโทษและประวัติอาชญากรรม ซึ่งกระทำโดยใช้ชื่อของเหยื่อในการก่ออาชญากรรม ทำให้เหยื่อมีประวัติทางอาญาและกลายเป็นผู้กระทำผิดโดยไม่รู้ตัว ส่งผลกระทบเป็นอย่างมากทั้งต่อภาครัฐ ภาคเอกชนและประชาชน เพราะการโจรกรรมอัตลักษณ์บุคคลสามารถที่จะขยายไปสู่การก่ออาชญากรรมในรูปแบบต่าง ๆ ได้อีกด้วย เนื่องจากสามารถเข้าถึงได้อย่างสะดวกในทุกพื้นที่ที่ต้องการ ดังนั้น ทุกคนและทุกภาคส่วนจึงจำเป็นต้องมีการสร้างความตระหนักรู้ในการปกป้องและป้องกันอัตลักษณ์บุคคล ทั้งต่อตนเองและบุคคลแวดล้อม เพื่อไม่ให้เกิดช่องโหว่และตกเป็นเหยื่อของอาชญากร อันจะนำมาซึ่งความเสียหายอย่างมากมาย ทั้งต่อตนเองรวมถึงระดับประเทศ สิ่งสำคัญที่สุดคือทุกคนจะต้องตระหนักรู้และให้ความสำคัญแก่อัตลักษณ์บุคคลของตนเองและเรียนรู้วิธีการในการใช้ชีวิตบนโลกแห่งอินเทอร์เน็ตที่ไร้พรมแดนอย่างรอบคอบและปลอดภัย ป้องกันตนเองไม่ให้ตกเป็นเหยื่อ ในขณะเดียวกันก็ปกป้องผู้อื่นที่อยู่แวดล้อม เพื่อให้ทุกคนสามารถใช้ชีวิตได้อย่างปลอดภัยและมีความสุขในสังคมออนไลน์

คำสำคัญ: โจรกรรมอัตลักษณ์บุคคล อัตลักษณ์บุคคล อาชญากรรมไซเบอร์ ภัยคุกคามไซเบอร์

Abstract

The objective of this study is to present identity theft in cyber which included structural forms, types of information, and the means to solve the problems of crimes. Nowadays the world becomes a place of information technology and borderless communication as the internet is connecting the world together, information technology, therefore plays a vital role in our daily life and becomes a part of our life. The internet can facilitate and respond to human needs to exchange the information between them which makes everyone trust in the system and expose their personal information to the public. Therefore, it is a loophole for criminals to access to the sensitive and confidential personal information including bank account information, credit information and taxation. These criminals would create fake accounts for their criminal purposes, for instance, driving license, passport, and etc. under the name of victims through the use of various tactics and modern technology as part of a tool to commit in crimes. This has a huge impact on the government, private sector, and the public because identity theft can be extended to various forms of crimes as it is easily accessible in all areas. Therefore, everyone and every sector need to raise an awareness to protect both oneself and their surrounding identity to narrow the loopholes and to avoid becoming a victim of such criminals. The most important thing is everyone must be aware and value their own identity and learn how to survive on the world of internet carefully and safely to protect oneself from becoming a victim and protect others to be safe and happy on the social networks and online communities

Keywords: Identity Theft, Identity, Cyber Crime, Cyber Threat

บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศเข้ามามีบทบาทต่อการดำเนินชีวิตประจำวันเป็นอย่างมาก จนเรียกได้ว่าเป็นส่วนหนึ่งของการดำรงชีวิต เพราะการใช้อินเทอร์เน็ตช่วยอำนวยความสะดวกและตอบสนองความต้องการของมนุษย์ได้ คนส่วนใหญ่จึงมักคิดว่าอินเทอร์เน็ตเป็นสิ่งที่ปลอดภัย ถูกต้อง และเที่ยงตรงในการใช้งาน เพื่อการแลกเปลี่ยนข้อมูลระหว่างกัน อาทิ ข้อมูลส่วนบุคคล หนังสือเดินทาง บัตรประจำตัวประชาชน หมายเลขประกันสังคม บัตรเครดิต และรหัสต่าง ๆ เมื่อมีการร้องขอ เช่น การจองโรงแรม การจองตั๋วเครื่องบิน การซื้อของออนไลน์ เป็นต้น ข้อมูลเหล่านี้จะถูกส่งจากคอมพิวเตอร์ของเราไปสู่ระบบอื่น ๆ ที่เป็นตัวรองรับในการจัดการ เพื่อให้ได้มาซึ่งสิ่งที่ต้องการ จึงทำให้ทุกคนมักจะเชื่อใจและไว้วางใจในการเปิดเผยข้อมูลส่วนบุคคลออกสู่สาธารณะ เพียงเพราะคิดว่าเป็นแค่การซื้อของ การสมัครสมาชิก ฯลฯ เท่านั้น และคิดว่าระบบที่ใช้จะมีความปลอดภัยและปกป้องสิทธิและข้อมูลส่วนบุคคลของตนได้

แต่ในความเป็นจริงอาชญากรมีอยู่ในทุกที่ทั่วโลก ไม่เว้นแม้แต่บนเครือข่ายไร้สายอย่างอินเทอร์เน็ต ข้อมูลต่าง ๆ สามารถบอกให้รู้ถึงอัตลักษณ์บุคคลของแต่ละคนได้เป็นอย่างดี เมื่อเทคโนโลยีพัฒนาอย่างต่อเนื่อง อาชญากรก็พัฒนาเช่นกัน การใช้เทคโนโลยีสมัยใหม่ในการก่ออาชญากรรม หรือที่ปัจจุบันเรียกว่า อาชญากรรมไซเบอร์เกิดขึ้นอย่างต่อเนื่อง ไม่ว่าจะเป็นการแฮ็ก (Hacking) ระบบคอมพิวเตอร์และอีเมล์ต่าง ๆ หรือที่เรียกว่า อีเมล์หลอกลวง (phishing) รวมไปถึงการเผยแพร่ข้อมูลออนไลน์ แฮ็กเกอร์มีความสามารถในการเข้าถึงได้

ทุกพื้นที่บนอินเทอร์เน็ตไม่ว่าเราจะอยู่ที่ไหนหรือทำอะไรก็ตาม พวกเขาสามารถเข้ามาจัดการและทำลายข้อมูลทั้งหลายบนเครื่องคอมพิวเตอร์ของเราได้โดยผ่านระบบอินเทอร์เน็ต ซึ่งปัจจุบันทุกเครื่องมักจะเชื่อมต่อกับอินเทอร์เน็ตอยู่เสมอและตลอดเวลา จึงทำให้เป็นหนทางที่ง่ายที่สุดในการจะได้มาซึ่งข้อมูลส่วนบุคคลที่ง่ายกว่าวิธีอื่น ๆ เพราะวิธีที่เข้าถึงตัวบุคคลเป็นวิธีที่ค่อนข้างเสี่ยงและอาจจะเกิดความผิดพลาดได้ อีกทั้ง ยังเป็นวิธีที่ทำให้ทราบว่าอาชญากรที่ก่อเหตุนั้นเป็นใคร และจะสามารถตามจับตัวได้อย่างรวดเร็วในที่สุด จึงทำให้อาชญากรหันไปใช้วิธีการก่ออาชญากรรมไซเบอร์ซึ่งง่าย สะดวก และรวดเร็วในการได้สิ่งที่ต้องการ นอกจากนี้ยังสามารถก่ออาชญากรรมในรูปแบบต่าง ๆ ได้อีก รวมถึงการกระทำเป็นองค์กรอาชญากรรมข้ามชาติ เพราะสามารถติดต่อสื่อสารกันด้วยระบบเครือข่ายและขยายองค์กรให้ใหญ่ขึ้น จึงทำให้การก่ออาชญากรรมเป็นไปโดยสะดวกและเข้าถึงได้ทุกพื้นที่ที่ต้องการ

ข้อมูลบุคคลจึงเป็นสิ่งสำคัญและจำเป็นอย่างมากในการดำรงชีวิต เพราะเป็นการบ่งบอกถึงตัวตนของบุคคลนั้น จึงทำให้เกิดการโจรกรรมข้อมูลบุคคล เพื่อนำไปใช้ก่ออาชญากรรม หรือที่เรียกว่า การโจรกรรมอัตลักษณ์บุคคล (Identity Theft) นั่นเอง

การโจรกรรมอัตลักษณ์บุคคล (Identity Theft)

การโจรกรรมอัตลักษณ์บุคคล เป็นอาชญากรรมที่เกิดขึ้นเป็นจำนวนมากในปัจจุบัน การโจรกรรมอัตลักษณ์บุคคลเกิดจากการที่มีบุคคลอื่นมาใช้ข้อมูลส่วนบุคคลของเรา โดยไม่ได้รับอนุญาตและความยินยอมในการใช้ซึ่งถือว่าเป็นสิ่งผิดกฎหมาย ปัจจุบันมีคนนับล้านได้รับผลกระทบทั้งทางตรงและทางอ้อมจากอาชญากรรมในรูปแบบนี้

การให้คำนิยามของการโจรกรรมอัตลักษณ์บุคคล มีมากมายจากหลากหลายแหล่ง อาทิ อาชญากรสามารถค้นหารายละเอียดส่วนบุคคลของคุณ และใช้มันเพื่อเปิดบัญชีธนาคารและบัตรเครดิต สินเชื่อ ผลประโยชน์ต่าง ๆ และเอกสารสำคัญ เช่น หนังสือเดินทาง ใบขับขี่ เป็นต้น การโจรกรรมอัตลักษณ์บุคคลยังสามารถอธิบายได้ว่าเป็นการนำข้อมูลส่วนบุคคลของผู้อื่นมาถ่ายโอน เพื่อกระทำการบางอย่างที่ผิดกฎหมายโดยไม่ได้รับการอนุญาต ซึ่งเป็นการละเมิดกฎหมายกลางของรัฐและผิดกฎหมายอาญาของท้องถิ่นของประเทศสหรัฐอเมริกา [1]

แต่ในบางครั้งก็ไม่ได้หมายถึงเรื่องของเงินแต่เพียงอย่างเดียว อาจโจรกรรมไปเพื่อวัตถุประสงค์อื่น เช่น สืบราชการลับ การก่อการร้าย การแก้แค้น หรือการอพยพอย่างผิดกฎหมาย [2] แต่อย่างไรก็ตาม มักจะยอมรับโดยทั่วไปว่า วัตถุประสงค์หลักจริง ๆ ของการโจรกรรมอัตลักษณ์บุคคลนั้น มักจะทำไปเพื่อผลประโยชน์ทางการเงิน ซึ่งเจอรัลด์และคณะได้ให้ความหมายไว้ว่า การโจรกรรมอัตลักษณ์บุคคลเป็นความผิดทางอาญาอย่างหนึ่งในการสมมติตัวตนของตนเป็นอีกคนหนึ่งซึ่งมีผลประโยชน์ที่เราต้องการ ผลประโยชน์ส่วนใหญ่มักจะเป็นเรื่องของการเงิน การทำธุรกรรมธนาคารต่าง ๆ รวมไปถึงการเข้าถึงข้อมูลเครือข่ายโทรศัพท์ หรือสาธารณูปโภคอื่น ๆ ที่ได้รับประโยชน์จากรัฐ [3]

การโจรกรรมอัตลักษณ์บุคคลเป็นอาชญากรรมที่มีความเสี่ยงต่ำ แต่ผลประโยชน์ที่ได้รับมีมูลค่าสูง ในขณะที่บทลงโทษไม่ได้รุนแรงเท่าที่ควร โดยปกติผู้ที่ถูกโจรกรรมข้อมูลส่วนบุคคลมักจะถูกขโมยชื่อ ที่อยู่ หมายเลขประกันสังคม และหมายเลขบัญชีเป็นหลัก แต่ยังมีข้อมูลอื่น ๆ อีกมากมายที่ถูกโจรกรรมเช่นกัน ซึ่งข้อมูลเหล่านี้ล้วนมีความสำคัญเป็นอย่างยิ่งเพราะถูกนำไปใช้ในทางไม่ถูกกฎหมาย

ลักษณะข้อมูลที่มักถูกโจรกรรม

CIPPIC ได้ทำการแบ่งประเภทของข้อมูลส่วนบุคคลที่ถูกโจรกรรมไว้ทั้งสิ้น 4 ประเภทใหญ่ [4] ได้แก่

ประเภทที่ 1 ข้อมูลส่วนบุคคลทั่วไป ได้แก่ ชื่อ ที่อยู่ สถานะ เพศ อายุ วันเกิด หมายเลขประกันสังคม ข้อมูลครอบครัว ข้อมูลการรักษาพยาบาล เป็นต้น

ประเภทที่ 2 ข้อมูลสินทรัพย์ เช่น บ้าน ยานพาหนะ ข้อมูลด้านสังหาริมทรัพย์และอสังหาริมทรัพย์ การจดทะเบียนทรัพย์สินต่าง ๆ เป็นต้น

ประเภทที่ 3 ข้อมูลทางการเงิน เช่น หมายเลขบัตรเครดิต บัตรเดบิต หมายเลขประจำตัวผู้เสียภาษี รายได้ หมายเลขบัญชีธนาคาร เป็นต้น

ประเภทที่ 4 ข้อมูลทางกายภาพ เช่น น้ำหนัก ส่วนสูง ลายนิ้วมือ เสียง เป็นต้น

จะเห็นได้ว่า ประเภทข้อมูลที่กล่าวมาล้วนเป็นสิ่งที่สามารถบ่งบอกถึงอัตลักษณ์ของบุคคลได้อย่างสมบูรณ์ จึงทำให้อาชญากรต้องการเป็นอย่างมาก เพื่อให้สามารถปลอมแปลงตัวตนเป็นบุคคลนั้น ๆ ในการทำบางอย่างที่ก่อให้เกิดความเสียหาย ดังนั้น ทั้งภาครัฐ ภาคเอกชน และประชาชน จึงจำเป็นต้องรู้วิธีป้องกันข้อมูลของตนเอง และรู้เท่าทันอาชญากร เช่น ด้านเทคนิคการโจรกรรม วิธีการ ตลอดจนความเสียหายที่เกิดขึ้นหากเกิดการโจรกรรม รวมถึงกฎหมายและแนวปฏิบัติต่าง ๆ

ประเภทของการโจรกรรมอัตลักษณ์บุคคล

การโจรกรรมอัตลักษณ์บุคคล อาชญากรจะกระทำขึ้นเพื่อวัตถุประสงค์บางอย่างที่ก่อให้เกิดประโยชน์แก่ตน แต่สร้างความเสียหายแก่ผู้ถูกกระทำ ซึ่งถือว่าเป็นความผิดทางอาญา สามารถแบ่งออกเป็น 3 ประเภทใหญ่ ๆ ได้แก่ [5]

1. การโจรกรรมข้อมูลทางการเงินในการใช้งานบัตรเครดิตเพื่อซื้อสินค้าหรือทำธุรกรรมทางการเงิน ซึ่งเป็นการโจรกรรมที่แพร่หลายมากที่สุด

2. การโจรกรรมข้อมูลอาชญากรรม เพื่อนำข้อมูลไปแจ้งแก่เจ้าหน้าที่ผู้บังคับใช้กฎหมายบังคับบุคคลนั้นให้มีความผิดทางอาญา โดยที่เขาเหล่านั้นอาจจะไม่ได้กระทำผิด

3. การโจรกรรมข้อมูลส่วนบุคคลด้วยวิธีการโคลนนิ่งข้อมูลขึ้นมาให้เหมือนกับต้นแบบ (Identity Cloning) การโคลนนิ่งทำได้ง่ายเมื่อเป็นการโจรกรรมข้อมูลของเด็ก เพราะประวัติของเด็กหรืออัตลักษณ์บุคคลของเด็กมักจะไม่ถูกตรวจสอบจากพ่อแม่ จนกระทั่งเด็กมีอายุอย่างน้อย 18 ปี จึงจะทำการตรวจสอบ เพราะโดยทั่วไปมักจะถือว่าไม่มีเหตุผลจำเป็นในการตรวจสอบเนื่องจากเด็กยังคงอยู่ในสายตาของพ่อแม่

การโจรกรรมอัตลักษณ์บุคคล อาชญากรสามารถเข้าถึงข้อมูลได้หลากหลายวิธี และด้วยวิวัฒนาการความก้าวหน้าของเทคโนโลยี จึงทำให้เกิดวิธีการต่าง ๆ ในการโจรกรรมข้อมูล เมอร์คิวรีได้อธิบายเพิ่มเติมว่า การโจรกรรมโดยทั่วไปสามารถทำได้ด้วยวิธีการ 2 แนวทางหลัก ๆ นั่นคือ Low-Tech และ Hi-Tech ซึ่งทั้ง 2 แนวทางมีทั้งข้อดีและข้อเสีย จึงจำเป็นจะต้องมีการตรวจสอบข้อมูลส่วนบุคคลของตนอย่างละเอียดและสม่ำเสมอ เพื่อป้องกันและตั้งรับเมื่อเกิดการโจรกรรม Low-Tech เป็นวิธีการที่เกิดขึ้นก่อนที่ยุคอินเทอร์เน็ตจะเข้ามา เป็นการโจรกรรมในรูปแบบเดิม ๆ ใช้การประชิดตัวหรือการโจรกรรมโดยตรงกับเหยื่อ ซึ่งมีโอกาสเกิดขึ้นมากกว่าวิธีการแบบ Hi-Tech หลายเท่า เทคนิคที่พบได้บ่อยคือ อาชญากรพยายามหาข้อมูลโดยการค้นหาจากถังขยะหรือตู้จดหมาย

ตามบ้าน หรือแม้แต่การบุกเข้าไปในบ้านหรือการทำลายรถยนต์ส่วนบุคคลเพื่อทำการโจรกรรม ซึ่งวิธีการที่ใช้มีมากมายขึ้นอยู่กับความชำนาญและช่ำชองของแต่ละคน เทคนิคที่อาชญากรใช้บ่อย ๆ [6] ได้แก่

Shoulder surfing เทคนิคนี้เป็นการให้บุคคลยืนด้านหลังของเหยื่อแล้วมองผ่านไหล่ของเหยื่อ โดยพยายามรวบรวมข้อมูลทั้งหมดจากเหยื่อ ยกตัวอย่างเช่น การพยายามมองรหัสผ่านโดยการยืนอยู่ด้านหลังเหยื่อเมื่อเหยื่อกำลังกดเงินจากตู้ ATM ซึ่งเหยื่อจะไม่รู้ตัวว่ากำลังเปิดเผยข้อมูลให้แก่คนอื่นโดยไม่ตั้งใจ

อีกเทคนิคหนึ่งที่ใช้กันอย่างแพร่หลาย คือ การพยายามทำให้ผู้ที่ตกเป็นเหยื่อนั้นจงใจเปิดเผยข้อมูลด้วยตนเอง ซึ่งวิธีนี้หลายคนอาจจะคิดว่าไม่ใช่วิธีการที่มีประสิทธิภาพมากนัก แต่ในความเป็นจริงแล้วกลับมีประสิทธิภาพมากกว่า เทคนิคนี้เรียกว่า Pretexting เป็นการใช้ข้อมูลบางส่วนของบุคคลเพื่อชักจูงหรือหว่านล้อมให้เปิดเผยข้อมูลมากขึ้นด้วยตนเอง ซึ่งวิธีการที่ใช้ส่วนมากจะใช้วิธีการโทรศัพท์ไปหาบุคคล แล้วอ้างว่าเป็นเจ้าหน้าที่จากธนาคารโทรศัพท์มา เพื่อแจ้งว่าเขากำลังตกเป็นเหยื่อและได้รับความเสียหายเป็นอย่างมาก จำเป็นจะต้องขอข้อมูลเพื่อดำเนินการต่อไป ซึ่งส่วนใหญ่เหยื่อมักจะหลงเชื่อและให้ข้อมูลทั้งหมดในที่สุด

แม้ว่าวิธีการแบบ Low-Tech ยังคงถูกใช้อยู่ในปัจจุบัน แต่ยังมีอีกวิธีการหนึ่งที่เรียกว่า Hi-Tech ถูกนำมาใช้มากขึ้นเช่นกัน จะเห็นได้ว่าวิธีการ Hi-Tech เป็นวิธีการที่ถูกนำมาใช้อย่างแพร่หลายและเพิ่มจำนวนขึ้นตลอดเวลา เพราะอาชญากรไม่จำเป็นต้องมีปฏิสัมพันธ์กับเหยื่อโดยตรง แต่สามารถรวบรวมข้อมูลหรือก่ออาชญากรรมได้โดยที่เหยื่อไม่รู้ตัว ซึ่งวิธีการ Hi-Tech มีเทคนิคที่หลากหลาย สามารถอธิบายได้ดังต่อไปนี้

Dumpster Diving/Trashing เป็นเทคนิคที่อาชญากรค้นหาขยะของเรา เพื่อตรวจสอบดูว่ามีข้อมูลส่วนบุคคลหรือไม่ ทั้งจากทางจดหมาย e-mail และอื่น ๆ ซึ่งโดยปกติแล้วมักจะไปค้นตามตู้รับจดหมายที่อยู่ตามบ้าน

อีเมล์หลอกลวง (Phishing) เทคนิคนี้จะใช้การแอบอ้างเป็นบริษัทหรือผู้มีอำนาจต่าง ๆ และจะส่ง e-mail ไปถึงเหยื่อโดยเป็นการส่งแบบเป็นทางการเพื่อร้องขอข้อมูลส่วนบุคคล เช่น การยืนยันหมายเลขบัญชีธนาคาร หมายเลขประกันสังคม หรือรหัสผ่าน โดยจะทำการส่ง e-mail ออกไปเป็นจำนวนมาก หรือที่เรียกว่า Spam เพื่อกระตุ้นให้เหยื่อเกิดความสนใจจนตกเป็นเหยื่อในที่สุด โดยปกติแล้ว e-mail แปลกปลอมหรือมาจากคนไม่รู้จักมักจะทำให้ผู้รับรู้สึกถึงความแปลกใจและจะต้องเปิดอ่านรายละเอียดใน e-mail และมักจะมี URL เพื่อให้กดเข้าไปยืนยันข้อมูลส่วนบุคคลโดยเฉพาะการกรอกรหัสผ่าน ซึ่ง e-mail จะถูกออกแบบให้คล้ายกับสถาบันการเงิน ขนาดใหญ่ เช่น ธนาคารต่าง ๆ PayPal บัตรเครดิต ในช่วงหลายปีที่ผ่านมาผู้คนเริ่มรู้เทคนิคในการโจรกรรมแบบนี้มากขึ้น จึงทำให้อาชญากรหรือที่เรียกว่า Phisher ได้เปลี่ยนเป้าหมายใหม่ โดยเปลี่ยนจากสถาบันการเงินขนาดใหญ่เป็นขนาดเล็กลงเพื่อเพิ่มจำนวนเหยื่อได้มากขึ้น [7]

Spyware เป็นโปรแกรมที่ถูกสร้างขึ้นเพื่อติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้ ซึ่งโปรแกรมนี้จะแสดงผลเมื่อผู้ใช้ได้ทำการกด URL ที่ถูกส่งมาใน e-mail หรือ URL แปลกปลอมที่มักจะขึ้นให้กดเวลาเราดูหนังตามเว็บไซต์ต่าง ๆ ซึ่งโปรแกรมนี้จะถูกควบคุมและสั่งการมาจากผู้คิดค้นเพื่อให้เก็บข้อมูลส่วนตัวของผู้ใช้ทั้งหมด ไม่ว่าจะเป็นหมายเลขบัญชี รหัสผ่าน และอื่น ๆ โดยที่ผู้ใช้ไม่รู้ตัว จากนั้นก็จะถูกนำไปก่ออาชญากรรมหรือเพื่อวัตถุประสงค์อื่นที่ขัดต่อกฎหมาย

Credit Card Skimming เป็นเทคนิคที่อาชญากรจะทำการค้นหา สืบค้น หรือขโมยบัตรเครดิตของเหยื่อเพื่อนำไปขายในตลาดมืด โดยเมื่อได้บัตรเครดิตแล้วจะทำการปลอมแปลงโดยใช้เลขเดิมเพื่อขายต่อให้ลูกค้า

จากนั้นลูกค้าก็จะนำไปใช้โดยที่เจ้าของบัตรเครดิตตัวจริงเป็นผู้รับผิดชอบทั้งหมด เช่น ซื้อของ กดเงินสดจากตู้ ATM โดยผ่านบัญชีของเหยื่อ เหยื่อจะรู้ตัวก็ต่อเมื่อมีการเรียกเก็บค่าใช้จ่าย หรือมีการแจ้งเตือนจากทางธนาคารถึงความผิดปกติที่เกิดขึ้น

วิลเลียม โรเบิร์ด และสเตซี่ แอล เชรฟ [8] ทำการศึกษาเกี่ยวกับการละเมิดข้อมูลและการโจรกรรมอัตลักษณ์บุคคล (Data Breaches and Identity Theft) เป็นการศึกษาเกี่ยวกับผลกระทบของการเก็บรวบรวมข้อมูลส่วนบุคคลและความปลอดภัยของข้อมูลเมื่อเกิดเหตุการณ์การโจรกรรมข้อมูล รวมถึงค่าความเสียหายที่เกิดขึ้นบนเครือข่ายระบบจ่ายเงิน ซึ่งพบว่าข้อมูลได้ถูกเก็บรวบรวมไว้จำนวนมากมาย แต่ระบบรักษาความปลอดภัยยังไม่สามารถครอบคลุมข้อมูลจำนวนมากได้ทั้งหมด และยังมีประสิทธิภาพไม่ดีเพียงพอในการป้องกันและรักษาข้อมูล จึงได้ทำการทดลองและสร้างเป็นแบบจำลองขึ้นจากสมมติฐานที่กำหนด เพื่อกำหนดให้ผู้ที่เข้าใช้ข้อมูลร่วมกันในแต่ละองค์กร โดยกำหนดผู้เข้าใช้และระบบรักษาความปลอดภัยฐานข้อมูล เพื่อป้องกันการถูกโจรกรรมทั้งจากภายนอกและภายในองค์กร เนื่องจากข้อมูลระบบการจ่ายเงินไม่ได้มีองค์กรเดียวในการทำงาน แต่ยังรวมหลายองค์กรอีกด้วย

ทางด้าน เฮธ คอร์ป, เคนท์ อาร์ เคอร์เลย์ และจอห์น เคน [9] ได้ศึกษาเรื่องของความแตกต่างของการโจรกรรมอัตลักษณ์บุคคล: การศึกษาเกี่ยวกับเหยื่อโดยการใช้แบบสำรวจเรื่องการตกเป็นเหยื่อแห่งชาติ (Differentiating identity theft: An exploratory study of victims using a national victimization survey) ซึ่งเป็นการศึกษาความแตกต่างของการโจรกรรมอัตลักษณ์บุคคลในแต่ละประเภท โดยจะเป็นการศึกษาเหยื่อจากแบบสำรวจของ National Public Survey on White Collar Crime ในแต่ละประเภทอาชญากรรม เพื่อดูมูลเหตุจูงใจและลักษณะของเหยื่อหรือผู้ถูกกระทำ เพื่อนำไปสู่การบังคับใช้กฎหมายได้อย่างถูกต้องตามประเภทของอาชญากรรม ซึ่งพบว่า บางครั้งการโจรกรรมอัตลักษณ์บุคคลไม่ได้รวมถึงการฉ้อโกงบัตรเครดิตแต่อย่างใดในบางการศึกษา แต่บางการศึกษาจะรวมเป็นประเภทเดียวกัน ทำให้การเก็บข้อมูลเป็นไปได้ยากเพราะไม่สอดคล้องกัน ดังนั้น จึงได้มีการศึกษาข้อมูลจากแบบสำรวจของ National Public Survey on White Collar Crime เพื่อนำมาวิเคราะห์ถึงระดับความรุนแรงของอาชญากรรม โดยดูจากลักษณะและความเสี่ยงที่เกิดขึ้นกับเหยื่อ อีกทั้งยังได้ทำการเปรียบเทียบเหยื่อแต่ละประเภทของอาชญากรรมที่เกิดขึ้นถึงมูลเหตุจูงใจในการตกเป็นเหยื่อของอาชญากรรมประเภทนี้ อาทิ การฉ้อโกงบัตรเครดิต การฉ้อโกงบัญชีธนาคาร และอื่น ๆ ซึ่งพบว่า โดยส่วนใหญ่แล้วบุคคลที่ตกเป็นเหยื่อจะเป็นผู้หญิง ผิวดำ คนหนุ่มสาว และมีรายได้น้อย ทำให้ตกเป็นเหยื่อของอาชญากรรมประเภทนี้ ซึ่งเมื่อเกิดการโจรกรรมข้อมูลส่วนบุคคลไปแล้วได้สร้างความเสียหายและประวัติไม่ดีแก่เหยื่อ เนื่องจากเหยื่อส่วนใหญ่จะถูกสวมรอย เพื่อนำข้อมูลไปใช้ในทางธุรกรรมทางการเงิน

ส่วนเอริค โฮล์ม [10] ได้ทำการศึกษาเรื่องเครือข่ายสังคมออนไลน์และการโจรกรรมอัตลักษณ์บุคคลในสังคมดิจิทัล (Social networking and identity theft in the digital society) เป็นการศึกษาเกี่ยวกับความเสี่ยงของผู้ใช้งานเครือข่ายสังคมออนไลน์กับการโจรกรรมอัตลักษณ์บุคคล เมื่อบุคคลนั้นเปิดเผยข้อมูลส่วนตัวบนสังคมออนไลน์ เช่น อายุ เพศ ที่อยู่ การศึกษา ภาพถ่าย และข้อมูลส่วนบุคคลอื่น ๆ ที่บ่งบอกถึงความเป็นตัวตน ซึ่งอาชญากรจะใช้ประโยชน์จากช่องโหว่ของสังคมออนไลน์ที่เกิดจากการเผยแพร่ข้อมูลส่วนบุคคล โดยการโจรกรรมข้อมูลของบุคคลอื่นเพื่อใช้ในการปลอมแปลง การฉ้อโกง และการก่ออาชญากรรมแต่ละประเภทตามที่ต้องการ ในขณะที่กลไกการป้องกันควบคุมได้ยาก เพราะเครือข่ายสังคมออนไลน์เป็นเครือข่ายไร้พรมแดนและเปิดกว้างอย่างเสรี ซึ่งการศึกษาในครั้งนี้เป็นการศึกษาจากเอกสาร งานวิจัย และวรรณกรรมจาก 3 ประเทศ ได้แก่ ออสเตรเลีย

สหรัฐอเมริกา และสหราชอาณาจักร โดยเน้นที่ความสำคัญของความสัมพันธ์ระหว่างเครือข่ายสังคมออนไลน์และการโจรกรรมอัตลักษณ์บุคคล รวมถึงการพัฒนาการสร้างความเข้าใจระหว่างความสัมพันธ์ของข้อมูลส่วนบุคคลกับอาชญากรรม แต่สิ่งที่ยากก็คือการใส่ใจในการป้องกันข้อมูลส่วนบุคคลของตนเองมีน้อยกว่าความต้องการในการแบ่งปันข้อมูล ซึ่งเป็นความเสี่ยงที่ทำให้เกิดอาชญากรรม จึงได้เสนอแนะวิธีการป้องกันการโจรกรรมอัตลักษณ์บุคคลจากเครือข่ายสังคมออนไลน์ โดยมีด้วยกันหลายวิธี เช่น การสร้างความร่วมมือของคนในสังคมเพื่อป้องกันข้อมูลส่วนบุคคลของตนเอง การปรับปรุงกฎหมายให้ทันสมัยและบทลงโทษที่รุนแรงเพื่อให้เกิดความเกรงกลัว แต่สิ่งที่สำคัญที่สุดคือการสร้างความตระหนักรู้และการให้ความสำคัญในการป้องกันข้อมูลของตนเองเพื่อลดความเสี่ยงการก่ออาชญากรรมที่จะเกิดขึ้น

แนวทางการป้องกันและปราบปรามการโจรกรรมอัตลักษณ์บุคคลบนโลกไซเบอร์

การโจรกรรมอัตลักษณ์บุคคลนั้น อาชญากรสามารถเข้าถึงข้อมูลสำคัญและเป็นความลับของบุคคลได้ไม่ว่าจะเป็นข้อมูลบัญชีธนาคาร ข้อมูลเครดิต การเสียภาษี ตลอดจนการนำข้อมูลไปสร้างเป็นบัญชีปลอมเพื่อทำธุรกรรมต่าง ๆ เช่น การทำใบขับขี่ สูติบัตร หนังสือเดินทาง หรือแม้แต่การกระทำผิดภายใต้ชื่อของเหยื่อเพื่อหลีกเลี่ยงการถูกลงโทษและประวัติอาชญากรรม โดยการใช้ชื่อของเหยื่อในการก่ออาชญากรรมทำให้เหยื่อมีประวัติทางอาญาและกลายเป็นผู้กระทำผิดโดยไม่รู้ตัว ซึ่งได้สร้างความหวาดกลัวและความรู้สึกไม่ปลอดภัยให้เกิดขึ้นจนกลายเป็นความเครียดและส่งผลต่อสภาพร่างกายและจิตใจของเหยื่อ ส่วนใหญ่เหยื่อมักจะเสียทรัพย์สินเงินทองเป็นจำนวนมาก เพราะไม่สามารถจับตัวผู้กระทำผิดได้ในระยะเวลาอันสั้น หรือกำลังก่ออาชญากรรมในขณะเดียวกันเหยื่อจะรู้ตัวว่าตกเป็นเหยื่อก็ต่อเมื่อได้เกิดความสูญเสียไปแล้วไม่ใช่ในทันทีทันใด

การโจรกรรมอัตลักษณ์บุคคลเป็นหนึ่งในอาชญากรรมทางเศรษฐกิจที่เติบโตอย่างรวดเร็ว ไม่ว่าจะเป็นในประเทศใหญ่ ๆ อย่างสหรัฐอเมริกา อังกฤษ ฝรั่งเศส และประเทศในเอเชีย เช่น ญี่ปุ่น จีน รวมถึงประเทศไทย อาชญากรรมประเภทนี้ไม่เพียงแต่สร้างความเสียหายให้แก่บุคคลหรือองค์กร แต่ยังสร้างความเสียหายระดับประเทศ ภาครัฐแต่ละประเทศจึงเล็งเห็นความสำคัญในการกำกับดูแลด้านการตรวจสอบ และระบุตัวตนของพลเมืองเพื่อป้องกันการปลอมแปลงและสร้างความเสียหายที่จะเกิดขึ้น เพราะอาชญากรส่วนใหญ่มักจะทำเป็นองค์กรอาชญากรรมข้ามชาติ ทำงานอย่างเป็นระบบเพื่อให้ได้มาซึ่งข้อมูลที่ต้องการ แล้วนำไปปลอมแปลงเพื่อนำไปสู่การก่ออาชญากรรมประเภทอื่น เช่น การค้ามนุษย์ แรงงานข้ามชาติ การค้าอาวุธ การค้ายาเสพติด การหลบหนีเข้าเมือง ฯลฯ ทำให้เกิดเป็นปัญหาในหลายด้านทั้งทางด้านเศรษฐกิจ สังคม ด้านการทูต ตลอดจนด้านความมั่นคงของประเทศ ซึ่งการเติบโตและวิวัฒนาการอย่างก้าวกระโดดของเทคโนโลยีที่ใช้ทำให้ไม่สามารถตั้งรับได้ทัน อีกทั้ง การโจรกรรมไม่ได้ทำเพียงบุคคลหรือกลุ่มบุคคลเท่านั้น แต่มักจะทำเป็นองค์กรอาชญากรรมข้ามชาติ จึงทำให้การสืบสวนสอบสวนเพื่อหาผู้กระทำผิดเป็นไปได้ยาก รวมถึงการปรับเปลี่ยนของสภาวการณ์ของโลกจึงทำให้กฎหมายหลายอย่างจำเป็นต้องเปลี่ยนตามเพื่อให้ทันต่อสถานการณ์

ผลกระทบจากการโจรกรรมอัตลักษณ์บุคคลได้ส่งผลโดยตรงทั้งภาครัฐ ภาคเอกชน และประชาชนในระยะยาว ทำให้เกิดการสูญเสียรายได้ ภาพลักษณ์ รวมถึงการสร้างความเชื่อมั่นที่เกิดขึ้นแก่นานาอารยะประเทศในการลงทุนและการสร้างความร่วมมือให้เกิดขึ้นได้ ทำให้รัฐจำเป็นต้องลงทุนทางด้านโครงสร้างพื้นฐาน และการ

รักษาความปลอดภัยระบบฐานข้อมูลเพิ่มมากขึ้น รวมถึงการหามาตรการป้องกันและแก้ไข และฟื้นฟูเยียวยาแก่เหยื่อ เพื่อให้สามารถลดโอกาสการสูญเสียที่จะเกิดขึ้น

นอกจากนี้ รัฐจำเป็นจะต้องสร้างความตระหนักรู้และความรับผิดชอบต่อการใช้สื่อสังคมออนไลน์ให้แก่ทุกคน ไม่เพียงเฉพาะผู้ที่ตกเป็นเหยื่อหรือเจ้าหน้าที่ผู้ปฏิบัติงานเท่านั้น เพราะการป้องกันอัตลักษณ์ของตนเองเป็นสิ่งสำคัญและจำเป็นที่ทุกคนต้องตระหนักรู้และปฏิบัติตามมาตรการต่าง ๆ เพื่อไม่ให้ตกเป็นเหยื่อหรือเป็นผู้เสียหาย การสร้างความตระหนักรู้ในการป้องกันตนเองในโลกออนไลน์จากอาชญากร จำเป็นจะต้องสร้างความตระหนักรู้ในทุกภาคส่วน ได้แก่

1. ความตระหนักรู้ต่อตนเอง อัตลักษณ์บุคคลคือทุกสิ่งทุกอย่างที่บ่งบอกความเป็นตัวตนของตนเอง เมื่อนำเข้าสู่สังคมออนไลน์แล้วถือว่าไม่เป็นความลับอีกต่อไป แต่ต้องรู้จักวิธีการและสร้างความตระหนักให้เกิดแก่ตนเองในการป้องกันก่อนเกิดเหตุ ปัจจุบันคนเรามักจะเปิดเผยเรื่องราวของตนเองผ่านสื่อสังคมออนไลน์เพื่อจุดประสงค์หลาย ๆ อย่างตามที่ได้กล่าวมาข้างต้น จะเห็นได้ว่าเมื่อข้อมูลเข้าสู่ระบบสังคมออนไลน์แล้วยากต่อการปกป้อง ส่วนใหญ่มักจะละเลยและไม่ระมัดระวังตัว จึงทำให้เกิดการโจรกรรมอัตลักษณ์บุคคลขึ้นโดยเฉพาะผ่านทางสื่อสังคมออนไลน์

2. ความตระหนักรู้ของภาครัฐ ต้องมีการสร้างความรู้ความเข้าใจในการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างดี โดยเฉพาะการเข้าใจในข้อกฎหมายต่าง ๆ ที่เกี่ยวข้อง การศึกษาถึงกรณีศึกษาหรือคดีที่เคยเกิดขึ้น เนื่องจากการโจรกรรมอัตลักษณ์บุคคลในประเทศไทยส่วนใหญ่จะเข้าข่ายกฎหมายที่เกี่ยวข้องกับการฉ้อโกง หลอกลวง ทำให้เสียทรัพย์สินเป็นส่วนใหญ่ จึงทำให้ไม่มีกรณีของความผิดฐานการโจรกรรมอัตลักษณ์บุคคลโดยตรง

การจัดฝึกอบรมเพื่อเพิ่มพูนความรู้และทักษะของเจ้าหน้าที่ก็มีส่วนสำคัญ เพราะในบางครั้งการดำเนินคดีพยานหลักฐานหรือวัตถุพยานที่ใช้ในการพิสูจน์หลักฐานไม่มีความน่าเชื่อถือ เนื่องจากการขาดการครอบครองวัตถุพยานตามหลักสากล ซึ่งเป็นการพิสูจน์ความเชื่อมโยงของพยานหลักฐานกับการกระทำความผิด ดังนั้นการฝึกอบรมจึงเป็นอีกทางหนึ่ง รวมถึงการมีระเบียบข้อบังคับที่ชัดเจนในการบันทึกหลักฐานตามลำดับเวลาเพื่อแสดงถึงรายละเอียดในแต่ละขั้นตอนและพิสูจน์การเชื่อมโยงหลักฐานดังกล่าวกับการกระทำความผิดนั้น ๆ เพราะหากขาดการต่อเนื่องของการครอบครองวัตถุพยาน เมื่อเข้าสู่กระบวนการยุติธรรมในชั้นศาล พยานหลักฐานย่อมไม่เป็นที่น่าเชื่อถือ

ภาครัฐจะต้องสร้างความสัมพันธ์ระหว่างประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีที่รวดเร็วและล้ำสมัยกว่าประเทศไทย และทำการสร้างเครือข่ายกับต่างประเทศให้ได้มากที่สุด เพื่อสร้างความร่วมมือทั้งทางยุโรป สหรัฐอเมริกา และเอเชีย รวมทั้งแลกเปลี่ยนความรู้และการทำงานระหว่างกัน ตลอดจนการสร้างเครือข่ายพันธมิตรในการประสานงานให้ความช่วยเหลือ โดยสร้างความร่วมมือกันทั้งภาครัฐ ภาคประชาชน และภาคเอกชนอย่างเป็นระบบ เพื่อช่วยให้การรวบรวมพยานหลักฐาน ข้อเท็จจริงต่าง ๆ ที่ยุ่งยากซับซ้อนให้สามารถทำงานได้อย่างรวดเร็ว มีประสิทธิภาพ และเข้าถึงข้อมูลได้โดยง่าย

3. ความตระหนักรู้ของสังคม ปัจจุบันเป็นโลกของการเชื่อมโยงสื่อสารอย่างไร้พรมแดนด้วยอินเทอร์เน็ต ดังนั้น ต้องสร้างความน่าเชื่อถือและความมั่นใจให้แก่ประชาชนว่า ข้อมูลที่เรื่องส่วนตัวที่อยู่บนอินเทอร์เน็ต จะมีความปลอดภัย และต้องสร้างความตื่นตัวในเรื่องของการคุ้มครองข้อมูลส่วนบุคคลกับสิทธิในการเข้าถึง มองให้เห็น

ถึงปัญหาที่จะเกิดขึ้น เช่น ข้อมูลที่อยู่บนอินเทอร์เน็ตถูกเก็บไว้ที่ใด ใครสามารถเข้าถึงได้นอกจากเจ้าของ เป็นต้น ซึ่งการคุ้มครองและสิทธิการเข้าถึงจำเป็นจะต้องสร้างความสมดุลระหว่างกัน โดยเน้นหลักความโปร่งใส ตรวจสอบได้ และทุกคนสามารถเข้าถึงข้อมูลได้มากที่สุด โดยที่ข้อมูลยังได้รับความคุ้มครองอย่างสูงสุดเช่นกัน รวมถึงการสร้างความตระหนักรู้ในการรับผิดชอบต่อสังคมเมื่อเกิดเหตุการณ์ต่าง ๆ ปัจจุบันเมื่อเกิดเหตุการณ์ที่น่าสนใจแก่คนทั่วไป มักจะเกิดการตามหาตัวบุคคลที่เป็นต้นเรื่องด้วยการเข้าถึงข้อมูลส่วนบุคคลแล้วนำออกมาเผยแพร่ หรือที่เรียกว่า การล่าแม่มด เกิดขึ้นในโลกของอินเทอร์เน็ต จึงทำให้เกิดการละเมิดสิทธิส่วนบุคคลมากยิ่งขึ้น และเป็นช่องโหว่ให้อาชญากรสามารถเข้าถึงและนำข้อมูลไปก่ออาชญากรรมได้ ดังนั้น สังคมจำเป็นต้องเรียนรู้ที่จะอยู่ด้วยกันและเคารพในสิทธิซึ่งกันและกัน เพื่อป้องกันไม่ให้เกิดการโจรกรรมอัตลักษณ์บุคคล หรือการนำข้อมูลส่วนบุคคลออกมาเผยแพร่ได้อย่างง่าย หรือแม้แต่ในภาคธุรกิจที่ใช้ข้อมูลของผู้บริโภคในการวิเคราะห์และประมวลผลเพื่อประโยชน์ทางธุรกิจก็เช่นกัน จำเป็นจะต้องทำตามมาตรฐานที่หน่วยงานที่เกี่ยวข้องเป็นผู้กำหนดในการคุ้มครองข้อมูลส่วนบุคคลตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562

บทสรุป

ปัจจุบัน การโจรกรรมอัตลักษณ์บุคคลถือเป็นหนึ่งในอาชญากรรมที่เพิ่มจำนวนมากขึ้นและทวีความรุนแรงมากยิ่งขึ้น เพราะเป็นหนึ่งในอาชญากรรมที่สามารถนำไปก่ออาชญากรรมประเภทอื่นต่อไปจนไปถึงอาชญากรรมข้ามชาติ อีกทั้ง เป็นอาชญากรรมที่สามารถเกิดขึ้นได้ทุกที่ทุกเวลาโดยผ่านอินเทอร์เน็ตและไม่สามารถระบุเจาะจงพื้นที่ที่แน่นอนของตัวอาชญากรได้ เพราะส่วนใหญ่มักจะอยู่ต่างประเทศเป็นหลัก และที่สำคัญคือผู้เสียหายมักจะไม่ต้องการเอาความ เนื่องจากไม่มั่นใจในกระบวนการยุติธรรมและไม่อยากเสียเวลาในการดำเนินการ รวมถึงผลกระทบที่เกิดขึ้นไม่ได้เกิดกับผู้เสียหายโดยตรง แต่มักจะเกิดกับเหยื่อที่ถูกอาชญากรหลอกอีกขั้นหนึ่ง และส่วนใหญ่มักจะเป็นเรื่องของการเสื่อมเสียชื่อเสียง แต่ไม่กระทบถึงความเสียหายที่เป็นมูลค่าแต่อย่างใด ดังนั้น ทุกคนและ ทุกภาคส่วนจำเป็นจะต้องสร้างความตระหนักรู้ในการป้องกันอัตลักษณ์บุคคลของตนเองและบุคคลรอบข้าง โดยต้องเริ่มจากตัวบุคคลจนไปถึงระดับประเทศ เพราะอัตลักษณ์บุคคลเป็นสิ่งที่บ่งบอกถึงตัวตนของบุคคลนั้นอย่างแท้จริง และสามารถนำไปใช้ประกอบการทำกิจกรรมหรือธุรกรรมต่าง ๆ ได้ โดยเฉพาะบนโลกอินเทอร์เน็ต ในระดับตัวบุคคล จะต้องรู้จักวิธีป้องกันตนเอง เช่น การตั้งรหัสผ่าน การใส่ลายน้ำ เป็นต้น ในระดับประเทศ เช่น การกำหนดแนวนโยบายและกลยุทธ์ในการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี การเตรียมความพร้อมของบุคลากรในการรองรับกับอาชญากรรมทางเทคโนโลยีในรูปแบบต่าง ๆ ที่จะเกิดขึ้น รวมถึงการเตรียมความพร้อมด้านระบบเทคโนโลยีสารสนเทศและอุปกรณ์ต่าง ๆ เป็นต้น เพราะความเสียหายที่เกิดขึ้นอาจจะไม่พียงแต่เฉพาะด้านชื่อเสียง แต่อาจรวมถึงภาพลักษณ์ของประเทศ ตลอดจนผลกระทบด้านอื่น ๆ เช่น ด้านสังคม ด้านเศรษฐกิจ ด้านความมั่นคงระหว่างประเทศ เป็นต้น ซึ่งจะส่งผลให้เกิดความเสียหายอย่างมากมายตามมา ดังนั้น ทุกคนจำเป็นจะต้องเรียนรู้ในการป้องกันอัตลักษณ์บุคคลของตนเอง และวิธีการอยู่ในโลกไร้พรมแดนผ่านอินเทอร์เน็ตอย่างระมัดระวัง และรอบคอบเพื่อไม่ให้เกิดเหตุอาชญากรรมดังที่กล่าวมา

เอกสารอ้างอิง

[1] Mercuri, R. T., “Scoping identity theft”, Communications of the ACM, 49(5), page 17-21, 2006.

[2] Graeme R. Newman, Megan M. McNally, Identity Theft Literature Review. Federal funds provided by the U.S. Department of Justice, 2005-TO-008, 2005

[3] Gregory J. Gerard, William Hillison, Carl Pacini, “ Identity theft: the US legal environment and organisations’ related responsibilities”, Journal of Financial Crime, Vol. 12 Issue: 1, pp.33-43, 2004.

[4] CIPPIC, “Working Paper No. 2 : Techniques Of Identity Theft” [Internet], Ottawa, Canadian Internet Policy and Public Interest Clinic (CIPPIC), 2007.

[5] Norum, P. S., & Weagley, R. O., “College Students, Internet Use, and Protection from Online Identity Theft”, Journal of Educational Technology Systems, 35(1), pp. 45-59, 2007.

[6] Haygood, R., & Hensley, R., “Preventing identity theft: New legal obligations for businesses”, Employment Relations Today (Wiley), 33(3), pp. 71-83, 2006.

[7] Cukier, W. & Levin, A. , Internet fraud and cybercrime. In F. Schmalleger & M. Pittaro (Eds.), Crimes of the Internet（pp. 251-279), 2009.

[8] William Roberds & Stacey L. Schreft, “Data Breaches and Identity Theft”, Presentations at the Federal Reserve Bank of Chicago, the 2008 Payments Workshop at the Bank of Canada, and the 2008 LAEF Conference on Payments and Networks at UC Santa Barbara., 2009.

[9] Heith Copes, Kent R. Kerley and John Kane., “Differentiating identity theft: An exploratory study of victims using a national victimization survey”, Journal of Criminal Justice, Volume 38, Issue 5, September–October 2010, pp. 1045-1052, 2010.

[10] Eric Holm, “ Social networking and identity theft in the digital society”, The International Journal on Advances in Life Sciences, 6 (3&4), pp. 157-166: ISSN 1942-2660, 2014.