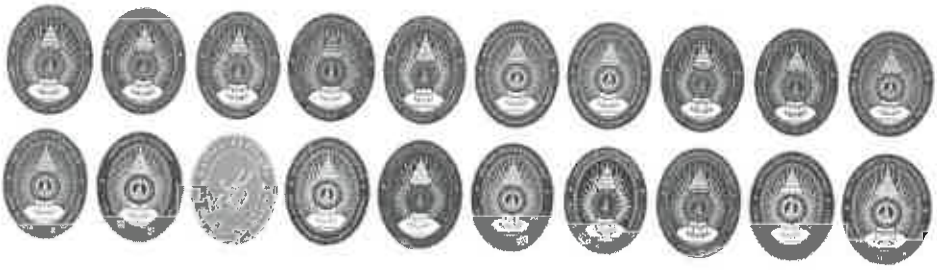

รายงานสืบเนื่องจากการประชุมวิชาการ

ระดับชาติ

ราชภัฏหมู่บ้านจอมบึงวิจัย

ครั้งที่ 9

ณ อาคารศูนย์ภาษาและคอมพิวเตอร์

มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง

วันจันทร์ที่ 1 มีนาคม 2564

สถาบันวิจัยและพัฒนา

มหาวิทยาลัยราชภัฏหมู่บ้านจอมบึง และเครือข่ายเจ้าภาพร่วม

สารบัญ

อาชญากรรมไซเบอร์: ภัยคุกคามรูปแบบใหม่ในบริบทประเทศไทย 4.0

Cyber Crime: New threats in the Context of Thailand 4.0

สุพล พรหมมาพันธุ์ [1]

[1] สาขาวิชาคอมพิวเตอร์ธุรกิจ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

สาระสังเขป

ปัจจุบัน ปัญหาอาชญากรรมไซเบอร์นับว่ามีความรุนแรงมากขึ้นตามลำดับ โดยเฉพาะในบริบทของประเทศไทย 4.0 ซึ่งเป็นนโยบายของรัฐบาลที่จะขับเคลื่อนเศรษฐกิจด้วยนวัตกรรมและเทคโนโลยีสารสนเทศ เพื่อยกระดับรายได้ของประชากร จากประเทศที่มีรายได้ปานกลาง ไปสู่ประเทศที่มีรายได้สูง รวมทั้งปัญหาเศรษฐกิจโลกที่กำลังหดตัวลงด้วยสาเหตุของโรคไวรัสโควิด 19 สำหรับความหมายของอาชญากรรมไซเบอร์ หรืออาชญากรรมทางคอมพิวเตอร์ (Cyber Crime) คือ การใช้เครื่องคอมพิวเตอร์ หรืออินเทอร์เน็ต เป็นเครื่องมือในการกระทำความผิดทางอาญาในลักษณะต่างๆ ได้แก่ การขโมย การเจาะระบบ การบุกรุก การแก้ไขทำลาย การเปลี่ยนแปลง การคัดลอก การปลอมแปลง การหลอกลวง รวมถึงการโจมตีด้วยไวรัส เป็นต้น สาเหตุส่วนหนึ่งที่เป็นปัจจัยทำให้เกิดอาชญากรรมไซเบอร์ ซึ่งเป็นภัยคุกคามรูปแบบใหม่ต่อระบบเศรษฐกิจของประเทศไทยและทั่วโลก คือ (1). สิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนมากขึ้น (2). ผู้ใช้งานคอมพิวเตอร์มีความคาดหวังต่อการใช้คอมพิวเตอร์สูงมาก และ (3). การขยายตัวและการเปลี่ยนแปลงของระบบเครือข่ายคอมพิวเตอร์ซึ่งเท่ากับเป็นความเสี่ยงใหม่ ส่วนรูปแบบของอาชญากรรมไซเบอร์ มีลักษณะดังต่อไปนี้ (1). การเข้าถึงเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต การแก้ไข การทำลายฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และทรัพยากรเครือข่าย (2).การคัดลอกหรือละเมิดลิขสิทธิ์ซอฟต์แวร์ (3).บุคคลผู้ไม่มีสิทธิ์เข้ามาแก้ไขข้อมูลสารสนเทศ (4).การขโมยฮาร์ดแวร์ ซอฟต์แวร์ สารสนเทศ และการขโมยเงินทางระบบอิเล็กทรอนิกส์ (5). การเจาะระบบและการบุกรุก (6). การโจมตีด้วยหนอน ม้าโทรจัน และไวรัส (7). การละเมิดทรัพย์สินทางปัญญา (8). การส่งไปรษณีย์อิเล็กทรอนิกส์ หรือข้อความไร้สาระ (สแปมมิ่ง) เพื่อรบกวนและสร้างความรำคาญเดือดร้อนให้กับผู้อื่น (9) การสมรู้ร่วมคิดในการใช้อุปกรณ์คอมพิวเตอร์ และเครือข่าย (10).การโกงการประมูล, การไม่ส่งสินค้าให้ลูกค้าตามใบสั่งซื้อ (11).การปลอมแปลงบัตรเครดิต และการหักเงินในบัญชี (12). การหลอกลวงทางอินเทอร์เน็ต เป็นต้น

คำสำคัญ : อาชญากรรมไซเบอร์ ประเทศไทย 4.0 การเจาะระบบ ทรัพย์สินทางปัญญา ไวรัส

SUMMARY

Today, Cyber Crime is becoming more and more serious, especially in the context of Thailand 4.0, which is the government's policy to drive the economy through Innovation and Information Technology, to raise the income of the population from middle-income countries to countries with high income, including the shrinking global economic problem with the cause of the COVID-19 outbreak. For the definition of Cyber Crime or Computer Crime (Cyber Crime) is the use of a computer or the Internet is a tool in criminal offenses of various kinds: theft, hacking, Invasion, remediation, destruction,

changing, copying, spoofing, fraud, virus attacks etc. Some of the reasons that cause Cyber Crime, This is a new type of threat to the economy of Thailand and around the world including (1). The computer environment is more complex (2). Computer users have very high expectations for computer use and (3). The expansion and transformation of computer network systems equates to new risks Cyber Crime model It has the following characteristics: (1). Unauthorized access to the computer, remediation, destruction of hardware, software, data and network resources. (2). Copying or pirating software. (3). Persons who do not have the right to edit information. (4). Theft of hardware, software, information and electronic money theft (5). Hacking and, Invasion (6). Worm attacks, Trojan horses and viruses (7). Intellectual property infringement (8). Send by electronic mail or nonsense messages (spamming) to annoy and annoy others (9) conspiracy to use computer equipment and networks, (10). Auction fraud, failure to deliver products to customers according to purchase orders. (11). Credit card counterfeiting and account debiting. (12). Internet fishing, etc.

Keywords : Cyber Crime Thailand 4.0 Hacking Intellectual Property Virus

บทนำ

ด้วยสถานการณ์ปัจจุบัน เราจะเห็นได้ว่า ปัญหาอาชญากรรมทางไซเบอร์มีความรุนแรงมากขึ้นตามลำดับ สาเหตุมาจากหลายปัจจัยไม่ว่าจะเป็นในเรื่องนโยบายประเทศไทย 4.0 ที่รัฐบาลต้องการจะขับเคลื่อนเศรษฐกิจของประเทศไทย ด้วยนวัตกรรม และเทคโนโลยีสารสนเทศ เพื่อยกระดับรายได้ของประชากรในประเทศจากประเทศที่มีรายได้ระดับปานกลางไปสู่ประเทศที่มีรายได้สูง ประกอบกับการหดตัวของเศรษฐกิจโลก การระบาดของโรคไวรัสโควิด-19 ทำให้หลายบริษัทเลิกจ้างพนักงาน และทำให้คนตกงานเป็นจำนวนมาก ในขณะเดียวกันก็ทำให้ประชากรทั่วโลกมีความยากจนเพิ่มมากขึ้น ด้วยสาเหตุดังกล่าวนี้ จึงทำให้คอมพิวเตอร์ เครือข่ายอินเทอร์เน็ต และสมาร์ทโฟน ตกเป็นเป้าหมายหลักของอาชญากรคอมพิวเตอร์อย่างหลีกเลี่ยงไม่ได้ เพราะปัจจุบัน การทำธุรกรรมต่างๆ โดยเฉพาะการทำธุรกรรมทางด้านการเงิน ล้วนแต่ต้องใช้เครื่องคอมพิวเตอร์ แท็บเล็ต และสมาร์ทโฟน เป็นส่วนใหญ่ ดังนั้น องค์กร และสถาบันทางด้านการเงิน ต้องหันมาให้ความสำคัญในการปกป้องความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศให้มากขึ้น เนื่องจากจะมีการสร้างผลกระทบที่เสียหายต่อระบบเศรษฐกิจโดยตรง ในบทความวิจัยของสุพล พรหมมาพันธุ์ (2563) เรื่อง **"ปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษาสถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล"** ได้รายงานว่า ตามที่ได้มีการดำเนินการศึกษาเกณฑ์การเปรียบเทียบบริษัทในสหรัฐอเมริกา โดยสถาบันโพนิมอน เมื่อเดือนกรกฎาคม ค.ศ. 2010 พบว่าการโจมตีทางไซเบอร์ได้กลายเป็นเหตุการณ์ที่เกิดขึ้นร่วมกัน แต่ละบริษัท รวม 45 บริษัท จากรายงานการศึกษายังพบอีกว่า บริษัทเหล่านั้น ได้ตกเป็นเหยื่อของการโจมตีอย่างน้อย 1 ครั้งต่อสัปดาห์ แสดงให้เห็นถึงการเพิ่มขึ้นของเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์ ที่มีการสำรวจองค์กรมากถึง 443 องค์กรในสหรัฐ ที่ส่งคืนตอบแบบสอบถาม ในปี ค.ศ. 2009 สำหรับในประเทศไทย มีรายงานจากหนังสือพิมพ์ "ประชาชาติธุรกิจ" (ฉบับออนไลน์) เมื่อวันที่ 19 มิถุนายน พ.ศ.2558 พบว่า สถิติข้อมูลภัยคุกคามไซเบอร์ที่รวบรวมโดย ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (ThaiCERT) พบว่า ปี พ.ศ.2557 ที่ผ่านมา มีการแจ้งเหตุภัยคุกคาม จำนวน 4,008 กรณี และ 3 อันดับแรก ได้แก่ การโจมตีด้วยโปรแกรมไม่พึงประสงค์ (Malicious Code) 40.1%

(1,735 กรณี) การหลอกลวงออนไลน์ (Fraud) เพื่อการได้มาซึ่งข้อมูลหรือทรัพย์สินของผู้อื่น 26.4% (1,010 กรณี) และการบุกรุก/เจาะระบบคอมพิวเตอร์จนสามารถดึงข้อมูลได้สำเร็จ (Intrusion) 19.8% (711 กรณี) ขณะที่ 5 เดือนแรกของปี พ.ศ.2558 มีการแจ้งแล้ว 1,797 กรณี อันดับแรกเป็นการโจมตีด้วยมัลแวร์ 644 กรณี การหลอกลวงออนไลน์ 503 กรณี ความพยายามบุกรุกเข้าระบบ 324 กรณี และเจาะระบบได้สำเร็จ 323 กรณี นอกจากนี้ ยังมียอดสถิติภัยคุกคาม ปี 2563 ล่าสุด ดังตารางด้านล่างต่อไปนี้

สถิติ ภัยคุกคาม ปี พ.ศ.2563 และประเภทภัยคุกคาม ซึ่งรายงานโดย ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) อ้างอิงตามเอกสาร ECSIRT.net project on cooperation and common statics.

ประเภทภัยคุกคาม / เดือน	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
1. เนื้อหาที่ไม่เหมาะสม (Abusive content)	0	0	1	1	0	1	0	0	0	0	0	0	3
2. ความพร้อมในการใช้งาน (Availability)	10	19	19	9	12	26	2	0	0	2	0	0	99
3. การฉ้อโกง (Fraud)	50	52	76	103	38	27	22	61	24	35	0	0	488
4. การรวบรวมสารสนเทศ (Information gathering)	3	0	9	3	1	8	6	6	2	1	0	0	39
5. ความมั่นคงปลอดภัยของสารสนเทศ (Information security)	11	0	0	1	4	10	0	2	0	2	0	0	30
6. ความพยายามบุกรุก (Intrusion Attempts)	22	30	6	3	5	6	2	10	23	4	0	0	111
7. การบุกรุก (Intrusions)	51	10	13	4	4	14	4	2	17	28	0	0	147
8. รหัสที่เป็นอันตราย (Malicious code)	84	101	94	91	84	77	22	23	26	40	0	0	642
9. ช่องโหว่ (Vulnerability)	31	27	1	3	109	109	94	14	7	14	0	0	409
10. อื่นๆ (Other)	1	0	0	0	0	0	0	0	0	0	0	0	1
รวม	263	239	219	218	257	278	152	118	99	126	0	0	1969

ตารางที่ 1 สถิติภัยคุกคามทางอินเทอร์เน็ต ประจำปี 2563

(ที่มา: https://www.thaicert.or.th, 2563)

เนื้อความ

การแข่งขันในยุคปัจจุบัน เป็นการแข่งขันกันทางด้านเศรษฐกิจเป็นสำคัญ เพราะไม่มีการทำสงครามกันเหมือนสมัยก่อน รัฐบาลประเทศต่างๆ ทั่วโลก จึงหันมาให้ความสำคัญในเรื่องเศรษฐกิจ และการกินดีอยู่ดีของประชาชน ด้วยการออกนโยบาย และการกำหนดยุทธศาสตร์ในการพัฒนาประเทศของตนในลักษณะที่แตกต่างกันไป สำหรับในประเทศไทย พลเอก ประยุทธ์ จันทร์โอชา นายกรัฐมนตรี ได้เคยประกาศให้ความสำคัญถึงเรื่อง **นโยบายประเทศไทย 4.0 (Thailand 4.0)** เอาไว้อยู่หลายครั้งด้วยกัน เกี่ยวกับเรื่องประเทศไทย 4.0 พงศ์สุข หิรัญพฤกษ์ (2561) ได้กล่าวเอาไว้เมื่อครั้งได้รับเชิญมาเป็นวิทยากรบรรยาย Tech Talk ในหัวข้อ **"Trend IT2018 Live สดทันที ที่มีเรื่องกับหนุ่มแบไต๋"** ณ มหาวิทยาลัยศรีปทุม ความว่า เบื้องหลังในเรื่องประเทศไทย 4.0 นี้ มาจากกระทรวงการคลัง สมัยเมื่อครั้งที่ ดร.สมคิด จาตุศรีพิทักษ์ เป็นรัฐมนตรี เป็นผู้คิดจุดประกายเรื่องประเทศไทย 4.0 (Thailand 4.0) ขึ้นมา ก่อนจะเป็นยุคประเทศไทย 4.0 นั้น มีวิวัฒนาการดังต่อไปนี้ โดยเริ่มจากยุค **Thailand 1.0 คือ ยุคเกษตรกรรม** เน้นไปที่การผลิตและ

การขายพืชพันธุ์การเกษตรเป็นหลัก อาทิ การขายพืชไร่ ขายข้าว ข้าวโพด ถั่ว มันสำปะหลัง ขายพืชผัก ไก่ เป็ด และสุกร เป็นต้น **ยุค Thailand 2.0 คือ ยุคอุตสาหกรรมเบา** เน้นไปที่เรื่องการผลิตสินค้าอุปโภคบริโภคที่มีน้ำหนักเบา ซึ่งเป็นการผลิตสินค้าที่มีต้นทุนการผลิตไม่สูงมากจนเกินไป ได้แก่ เสื้อผ้าเครื่องนุ่งห่ม เครื่องดื่ม อาหารกระป๋อง กระเป๋า รองเท้า เครื่องเวชภัณฑ์และยา การผลิตเครื่องเล่นวิทยุ โทรทัศน์ ของเด็กเล่น รวมทั้งแป้งอีกหลากพลายชนิด เป็นต้น ต่อมาเป็น **ยุค Thailand 3.0 ยุคอุตสาหกรรมหนัก** โดยเน้นมาในเรื่อง การผลิตสินค้าอุตสาหกรรมหนักและการส่งออก ได้แก่ การผลิตขั้นสูง ได้แก่ การผลิตเหล็กกล้า ปูนซีเมนต์ การผลิตชิ้นส่วนยานยนต์ แผงวงจรไฟฟ้าอิเล็กทรอนิกส์ การผลิตฮาร์ดดิสก์ไดร์ฟ ก๊าซธรรมชาติ การกลั่นน้ำมัน เป็นต้น นอกจากนั้น ยังเน้นการเชิญชวนนักลงทุนต่างประเทศให้มาลงทุนภายในประเทศ และขยายการลงทุนไปยังต่างประเทศอีกด้วย สุดท้าย **ยุค Thailand 4.0 คือ เป็นยุควิสัยทัศน์เชิงนโยบายของรัฐบาล** โดยเน้นรูปแบบการพัฒนาเศรษฐกิจของประเทศไทยตามหลักแนวคิดที่ว่า **"มั่นคง มั่งคั่ง และยั่งยืน"** ทั้งนี้ เพื่อรองรับการเปลี่ยนแปลงของกระแสโลกที่มีการเปลี่ยนแปลงไปอย่างรวดเร็ว ซึ่งต้องทำให้ประเทศไทยต้องเร่งพัฒนานวัตกรรม และเทคโนโลยีสารสนเทศใหม่ๆ ขึ้นมา เพื่อยกระดับรายได้ของประชากรในประเทศจากประเทศที่มีรายได้ปานกลาง ไปสู่ประเทศที่มีรายได้สูง **ส่วนที่เรียกว่า 4.0 นั้น** เพราะว่าไปสอดคล้องข้องกับนโยบายของประเทศเยอรมนี ที่เป็นศูนย์กลางของประเทศยุโรป ซึ่งเขาได้พัฒนาประเทศเยอรมันเข้าสู่อุตสาหกรรม 4.0 แล้ว โดยเขาเรียกว่า **อุตสาหกรรม 4.0 (Industry 4.0)** หรือบางครั้งเรียกว่า **การเรียนรู้ของเครื่องจักรกล (Machine Learning)** อันหมายถึง การสอนให้เครื่องจักรกลสามารถเรียนรู้ได้ด้วยตนเอง คิดแทน และคิดต่อได้อีกด้วย

ในลำดับต่อมาเป็นเรื่องของสาเหตุ หรือปัจจัยทำให้เกิดอาชญากรรมไซเบอร์ ในหนังสือของ George W. Reynolds. (2012) เรื่อง Ethics in Information Technology ได้จำแนกออกเป็น 3 ประเด็น ดังต่อไปนี้ คือ (1). สิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนมากขึ้น (2). ผู้ใช้งานคอมพิวเตอร์มีความคาดหวังต่อการใช้คอมพิวเตอร์สูงมาก และ (3). การขยายตัวและการเปลี่ยนแปลงของระบบเครือข่ายคอมพิวเตอร์ซึ่งเท่ากับเป็นความเสี่ยงใหม่ และสอดคล้องกับรายงานวิจัยของพิมพ์ธรา พัสดุประดิษฐ์ ที่กล่าวถึงทฤษฎีสามเหลี่ยมอาชญากรรม (Crime Triangle Theory) โดยอธิบายถึงสาเหตุ และองค์ประกอบของการเกิดอาชญากรรมว่ามี 3 ด้านคือ (1). ผู้กระทำความผิด/คนร้าย (Offender) หมายถึง ผู้ที่มีความต้องการ (Crave) จะก่อเหตุหรือต้อง การลงมือกระทำความผิด (2). เหยื่อ (Victim)/เป้าหมาย (Target) หมายถึง บุคคล สถานที่ หรือวัตถุสิ่งของที่ถูกมุ่งหมายกระทำต่อ หรือเป็นเป้าหมายที่ต้องการกระทำผิด (3). โอกาส (Opportunity) หมายถึง ช่วงเวลา (Time) และสถานที่ (Place) ที่เหมาะสมที่ ผู้กระทำผิดหรือคนร้าย มีความสามารถจะลงมือกระทำความผิดหรือก่ออาชญากรรม สำหรับปัจจัยทำให้เกิดอาชญากรรมไซเบอร์ สามารถอธิบายรายละเอียดได้ดังต่อไปนี้

(1). สิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนมากขึ้น หมายความว่า สิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนเกิดขึ้นอย่างมากมาย ได้แก่ เครือข่ายคอมพิวเตอร์ เครื่องคอมพิวเตอร์ การปฏิบัติการ ระบบ การประยุกต์ใช้ เว็บไซต์ สวิตช์ เราเตอร์ และเกตเวย์ ที่เชื่อมต่อกัน และมีแรงผลักดันจากหลายร้อยล้านเส้นทางของรหัสการเขียนโปรแกรม สิ่งแวดล้อมของความซับซ้อนทางคอมพิวเตอร์เหล่านี้ ยังคงมีเพิ่มมากขึ้นอย่างต่อเนื่องทุกวัน จำนวนตัวเลขของเครือข่ายคอมพิวเตอร์ที่เชื่อมต่อเข้ามายังมีการขยายตัวเพิ่มมากขึ้นอย่างต่อเนื่องตัวอย่างเช่น การเชื่อมต่อจากอุปกรณ์ต่างๆ อย่างมากมาย ไม่ว่าจะเป็นคอมพิวเตอร์ส่วนบุคคล (Personal Computer: PC) แท็บเล็ต สมาร์ทโฟน เป็นต้น ในขณะเดียวกันก็มีการละเมิดความปลอดภัยทางด้านคอมพิวเตอร์อย่างต่อเนื่องด้วยเช่นกัน นอกจากนี้ องค์กรและพนักงานเป็นจำนวนมากหันมาใช้คอมพิวเตอร์การประมวลผลแบบกลุ่มเมฆ (Cloud computing) ในการทำงานและใช้ในการจัดเก็บข้อมูลการให้บริการผ่านอินเทอร์เน็ต เช่น Google Drive, One Drive, Drop Box, Amazon Cloud เป็นต้น และซอฟต์แวร์เสมือนจริงก็เช่นเดียวกัน ซอฟต์แวร์เสมือนจริงเป็นซอฟต์แวร์ที่เลียนแบบการทำงานของคอมพิวเตอร์

ฮาร์ดแวร์โดยสามารถปฏิบัติการได้หลายระบบที่ทำงานอยู่บนคอมพิวเตอร์แม่ข่ายที่เดียว ด้วยสถานการณ์ดังกล่าวนี้ ทำให้ยากต่อการควบคุมความมั่นคงปลอดภัย

(2). ผู้ใช้คอมพิวเตอร์ มีความคาดหวังต่อการใช้คอมพิวเตอร์สูงมากขึ้น เนื่องจากปัจจุบันนี้ เวลาเป็นเงินเป็นทอง คอมพิวเตอร์มีความเร็วมากขึ้น ผู้ใช้สามารถแก้ปัญหาเองได้ ในอนาคตไม่ช้านี้ ผู้ใช้สามารถที่จะผลิตได้เอง ด้วยเหตุผลดังกล่าวนี้ คนทำงานคอมพิวเตอร์ที่แผนกช่วยเหลือ (Help Desks) ต้องตกอยู่ภายใต้แรงกดดันในการที่จะให้คำตอบจากผู้ใช้ที่ร้องขอข้อมูลเข้ามาอย่างรวดเร็ว จากภายใต้แรงกดดันที่ว่านี้ บางครั้ง พนักงานคอมพิวเตอร์ที่แผนกช่วยเหลือ มีการลืมตรวจสอบไอดีของผู้ใช้ (users' IDs) หรือ ลืมตรวจสอบการอนุญาตสิทธิ์การใช้รหัสผ่าน และผู้ใช้คอมพิวเตอร์บางคน ได้แบ่งปัน ไอดีการเข้าสู่ระบบ และรหัสผ่าน (login IDs and Passwords) ทำให้ผู้ไม่ประสงค์ดีนำรหัสผ่านเหล่านั้น ไปใช้ในการแสวงหาผลประโยชน์ในทางที่มิชอบ โดยเฉพาะผลประโยชน์ทางด้านการเงิน

(3).การขยายตัวและการเปลี่ยนแปลงระบบเครือข่ายคอมพิวเตอร์ ซึ่งเท่ากับการมีความเสี่ยงใหม่ ธุรกิจได้เคลื่อนย้ายจากยุคของการใช้เครื่องคอมพิวเตอร์ทำงานเครื่องเดียว ซึ่งมีการการเก็บข้อมูลที่สำคัญไว้ในคอมพิวเตอร์เมนเฟรมแยกไว้ในห้องจัดเก็บ จนต่อมาได้เข้าสู่ยุคที่คอมพิวเตอร์ส่วนบุคคลที่เชื่อมต่อกับเครือข่ายคอมพิวเตอร์อื่นๆ ที่มีจำนวนนับล้านๆ เครื่องที่มีความสามารถในการใช้ข้อมูลร่วมกัน ที่เรียกว่าเป็นยุคของเครือข่าย (Network Era) และคอมพิวเตอร์ที่เชื่อมต่อกันด้วยอินเทอร์เน็ตทั้งหมดเหล่านั้น สามารถแบ่งปันสารสนเทศร่วมกันได้ ไม่ว่าจะเป็นคอมพิวเตอร์ แท็บเล็ต หรือสมาร์ทโฟน ที่มีการใช้งานแฟลตฟอร์มต่างๆ เช่น Facebook, Line, Twitter, YouTube หรือแม้กระทั่งแอปพลิเคชันทางด้านการเงินต่าง เช่น เป๋าตังค์ เป็นต้น ซึ่งการใช้งานอินเทอร์เน็ต และแอปพลิเคชันเหล่านี้ มีสถิติการใช้งานเพิ่มมากขึ้นอย่างก้าวกรโดด เมื่อกล่าวถึงเรื่องของเทคโนโลยีสารสนเทศ ซึ่งในปัจจุบัน เราสามารถพบเห็นได้โดยทั่วไป ทุกคนต่างยอมรับโดยดุษฎีว่า เทคโนโลยีสารสนเทศถือว่าเป็นเครื่องมืออันทรงพลังอย่างหนึ่ง ซึ่งมีส่วนช่วยผลักดันทำให้องค์กรประสบความสำเร็จตามเป้าหมายที่ได้วางเอาไว้ และด้วยความเจริญก้าวหน้าของเทคโนโลยีสารสนเทศนี่เอง ทำให้มีความยากเพิ่มขึ้นในการที่จะทำให้การเปลี่ยนแปลงเทคโนโลยีนำมาปรับให้เข้ากันได้

ดังนั้น เมื่อถึงคราวจะใช้คอมพิวเตอร์และอินเทอร์เน็ต ควรจะต้องมีวิธีการป้องกันความมั่นคงปลอดภัยในการใช้อินเทอร์เน็ตให้ดีเสียก่อนโดยเฉพาะการใช้จุดเชื่อมโยงสาธารณะ (Public Hotspot) เนื่องจากกิจกรรมการใช้อินเทอร์เน็ตเหล่านั้น อาจมีคนสอดแนม (Snooping) อยากรู้อยากเห็นความเคลื่อนไหวต่างๆ โดยเฉพาะกิจกรรมธุรกรรมทางด้านการเงิน ในเว็บไซต์ hotspotshield.com ซึ่งเป็นเว็บไซต์ที่บริการซอฟต์แวร์ที่เป็นประโยชน์ (Software Utility) ใช้สำหรับจัดเก็บข้อมูลต่างๆ ทั้งนี้ เพื่อให้แน่ใจว่า ข้อมูลของคุณทั้งหมดที่ถูกส่งไปบนอินเทอร์เน็ตตลอดจนถึงเครือข่ายเสมือนจริงส่วนบุคคล (Virtual Private Network : VPN) วีพีเอ็น คือ เส้นทางความปลอดภัยของอินเทอร์เน็ต มีบริษัทใหญ่ๆ จำนวนมาก ใช้ในการป้องกันข้อมูลที่ไวต่อการสัมผัส การใช้วีพีเอ็นเป็นเกราะป้องกันข้อมูล (Shields your data) จากบุคคลผู้ต้องการอยากรู้อยากเห็น เช่น สารสนเทศที่คุณกรอกแบบฟอร์ม, ข้อมูลบัตรเครดิต, การส่งข้อความรีบด่วน และกิจกรรมของเว็บเบราว์เซอร์ ดังนั้น ปัจจุบันจึงมีการติดตั้งเกราะป้องกันที่จุดเชื่อมโยง และเพิ่มระดับการป้องกันความมั่นคงปลอดภัยของสารสนเทศ

สำหรับสถิติพฤติกรรมการใช้อินเทอร์เน็ตของคนไทย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) หรือ ETDA (เอ็ตด้า) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เผยผลการสำรวจพฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี 2562 หรือ Thailand Internet User Behavior 2019 ชี้ ทศวรรษที่ผ่านมา คนไทยใช้อินเทอร์เน็ตเพิ่มขึ้นอย่างก้าวกระโดดกว่า 150% ส่งผลให้ปัจจุบันไทยมีผู้ใช้อินเทอร์เน็ต 47.5 ล้านคน หรือราว 70% ของจำนวนประชาชนทั้งหมด

ภาพที่ 1 พฤติกรรมผู้ใช้อินเทอร์เน็ตในประเทศไทย ปี พ.ศ.2562
(ที่มา https://www.etda.or.th, 2563)

จากการสำรวจข้อมูลของประชาชนเกี่ยวกับพฤติกรรมการใช้อินเทอร์เน็ต ประจำปี 2562 ผ่านทางออนไลน์ ช่วงเดือน ส.ค.- ต.ค. 2562 โดยมีคนไทยเข้ามาตอบแบบสอบถามกว่า 17,242 คน ซึ่งจากการวิเคราะห์ข้อมูล พบว่า ปี 2562 คนไทยใช้อินเทอร์เน็ตเฉลี่ยวันละ 10 ชั่วโมง 22 นาที เพิ่มขึ้น 17 นาทีจากปี 2561 และเมื่อพิจารณาเป็นรายประเด็นเทียบกับชั่วโมงการใช้งาน พบข้อมูล ดังนี้

ภาพที่ 2 พฤติกรรมชั่วโมงการใช้อินเทอร์เน็ตของคนไทย ปี พ.ศ.2562
(ที่มา https://www.etda.or.th, 2563)

ส่วนรูปแบบของอาชญากรรมไซเบอร์ มีลักษณะดังต่อไปนี้ (1). การเข้าถึงเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต การแก้ไข การทำลายฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และทรัพยากรเครือข่าย (2).การคัดลอกหรือละเมิดลิขสิทธิ์ซอฟต์แวร์ (3).บุคคลผู้ไม่มีสิทธิ์เข้ามาแก้ไขข้อมูลสารสนเทศ (4).การขโมยฮาร์ดแวร์ ซอฟต์แวร์ สารสนเทศ และการขโมยเงินทางระบบอิเล็กทรอนิกส์ (5). การเจาะระบบและการบุกรุก (6). การโจมตีด้วยหนอน ม้าโทรจัน และไวรัส (7). การละเมิดทรัพย์สินทางปัญญา (8). การส่งไปรษณีย์อิเล็กทรอนิกส์ หรือข้อความไร้สาระ (สแปมมิ่ง) เพื่อรบกวนและสร้างความรำคาญเดือดร้อนให้กับผู้อื่น (9) การสมรู้ร่วมคิดในการใช้อุปกรณ์คอมพิวเตอร์ และเครือข่าย (10).การโกงการประมูล, การไม่ส่งสินค้าให้ลูกค้าตามใบสั่งซื้อ (11).การปลอมแปลงบัตรเครดิตและการหักเงินในบัญชี (12). การหลอกลวงทางอินเทอร์เน็ต เป็นต้น และขอกล่าวรายละเอียดในแต่ละลักษณะ ดังต่อไปนี้

(1). การเข้าถึงเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต การแก้ไข การทำลายฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และทรัพยากรเครือข่าย การเข้าถึงคอมพิวเตอร์โดยไม่ได้รับอนุญาตในปัจจุบัน สามารถเข้าถึงได้ง่าย เนื่องจากผู้ใช้บางคนใช้อุปกรณ์คอมพิวเตอร์หลายเครื่อง บางคนอาจมีทั้งโน้ตบุ๊คคอมพิวเตอร์ แท็บเล็ต และสมาร์ทโฟน และอาจมีการใช้งานแบบขาดความระมัดระวัง เช่น เปิดอีเมล หรือเฟซบุ๊ก ค้างเอาไว้ และไม่ได้ Logout ออกจากระบบ หรือแม้บางครั้ง ผู้ที่เป็นเจ้าของเครื่องคอมพิวเตอร์ มีมาตรการป้องกันใส่รหัสป้องเอาไว้แล้ว แต่มีผู้ไม่ประสงค์ดีใช้ความพยายามเข้ามาแก้ไข ทำลายฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และทรัพยากรเครือข่ายในลักษณะต่างๆ ซึ่งการกระทำเหล่านี้ มีความผิดตาม พ.ร.บ. คอมพิวเตอร์ ปี พ.ศ.2550 แก้ไขปรับปรุง ปี พ.ศ.2560 มาตรา 5 ความว่า ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน มีโทษจำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 10,000 บาท ในงานวิจัยของธนนท์ทัส สุธริยานิติภักดี (2563) เรื่อง "อาชญากรรมคอมพิวเตอร์กรณีศึกษามาตรการป้องกันการเข้าถึงข้อมูลทางอินเทอร์เน็ตโดยมิชอบ" ได้รายงานว่า ผลการศึกษาพบว่าสถานการณ์ของปัญหามีปัญหามาก เช่น ภัยคุกคามจากมัลแวร์ ไวรัส การทำฟิชชิ่ง หรือการหลอกลวงทางอินเทอร์เน็ต และมีความยุ่งยากสลับซับซ้อน เนื่องมาจากมีจำนวนผู้ใช้บริการอินเทอร์เน็ตเพิ่มขึ้นเป็นจำนวนมากจากปีที่ผ่านมาสืบเนื่องจากอินเทอร์เน็ตเป็นเครือข่ายที่สื่อสารติดต่อถึงกันได้สะดวกรวดเร็ว ลักษณะและรูปแบบของปัญหาการเข้าถึงข้อมูลทางอินเทอร์เน็ตแบ่งได้ 2 ทางคือ 1)โดยทางตรงก็คือ จะโดนภัยคุกคามจากมัลแวร์หรือโปรแกรมประสงค์ร้าย ประเภทไวรัสคอมพิวเตอร์เจาะระบบหรือลักลอบเข้าสู่ระบบข้อมูลทางคอมพิวเตอร์บนเครือข่ายเข้ามาสร้างความเสียหายและ 2) โดยทางอ้อม ก็คือ การทำฟิชชิ่งร่วมกับเทคนิคการปฏิสัมพันธ์ทางสังคม ปัญหาและอุปสรรคของมาตรการป้องกันการเข้าถึงข้อมูลทางอินเทอร์เน็ตโดยมิชอบ

(2).การคัดลอกหรือละเมิดลิขสิทธิ์ซอฟต์แวร์ สำหรับเรื่องการคัดลอก และการละเมิดลิขสิทธิ์ซอฟต์แวร์ในที่นี้ยังมีความหมายรวมไปถึงเรื่องของการปลอมแปลงซอฟต์แวร์ด้วย ซึ่งทำให้ประเทศสูญเสียรายได้ การคัดลอกและการปลอมแปลงซอฟต์แวร์ที่มีการละเมิดลิขสิทธิ์ ส่วนใหญ่ที่พบ คือ Windows Server, Windows XP Professional, Windows 7 และ Microsoft Office 2010 ส่วนหนึ่งผลิตจากประเทศจีน

(3).บุคคลผู้ไม่มีสิทธิ์เข้ามาแก้ไขข้อมูลสารสนเทศ บุคคลผู้ไม่มีสิทธิ์ อาจจะเป็นญาติพี่น้อง คนรู้จัก หรือบุคคลภายนอกที่ไม่รู้จัก ผู้ดูแลระบบ ต้องมีการกำหนดสิทธิ์การเข้าถึงระบบสารสนเทศให้เหมาะสมเกี่ยวกับระดับความสำคัญว่า ข้อมูลชนิดใด ที่บุคคลทั่วไปสามารถเข้าถึงได้ และข้อมูลที่ชนิดใด ที่บุคคลภายนอกที่ไม่มีสิทธิ์การเข้าถึงได้ โดยผู้ดูแลระบบสามารถกำหนดได้ ตั้งแต่การป้อนข้อมูล การสร้างข้อมูล การแก้ไขข้อมูล การลบข้อมูล การอ่านได้อย่างเดียว การอนุมัติ รวมถึงการไม่มีสิทธิ์เข้าถึงข้อมูล เป็นต้น

(4).การขโมยฮาร์ดแวร์ ซอฟต์แวร์ สารสนเทศ และการขโมยเงินทางระบบอิเล็กทรอนิกส์ สำหรับการขโมยฮาร์ดแวร์ ซอฟต์แวร์ สารสนเทศ ได้แก่ การขโมยอุปกรณ์คอมพิวเตอร์ เช่น คีย์บอร์ด ซีพียู เมาส์ เคส (Case) หรือแม้กระทั่ง อุปกรณ์ฉายภาพ (Projector) โดยเฉพาะสถาบันการศึกษา โรงเรียน จะมีข่าวเรื่องการถูกขโมยเครื่องคอมพิวเตอร์ เพื่อเอาไปขายเกิดขึ้นอยู่เป็นระยะๆ ดังนั้น มหาวิทยาลัยบางแห่ง จึงต้องมีการติดตั้งกล้องวงจรปิดในห้องปฏิบัติการคอมพิวเตอร์ (LAB) เพื่อเฝ้าระวังปัญหาเกี่ยวกับการขโมยอุปกรณ์ฮาร์ดแวร์ ส่วนเรื่องการขโมยซอฟต์แวร์ ถ้าในสมัยก่อนๆ มักมีการจัดเก็บข้อมูลกันไว้ในแผ่นดิสก์เก็ต แฟลชไดร์ฟ หรือแม้กระทั่งเอ็กเทอร์นอลฮาร์ดดิสก์ (External Hard Disk) ซึ่งในขณะเดียวกันอาจมีสารสนเทศ ข้อมูลที่เป็นความลับอยู่ในนั้นด้วย สำหรับการขโมยเงินอิเล็กทรอนิกส์ เป็นเหตุการณ์จริงที่เคยเกิดขึ้นกับธนาคารไทย จากการรายงานข่าวของ**ทีมข่าวการเงินโพสต์ทูเดย์** (2563). รายงานว่า สองเหตุการณ์ที่ธนาคารกสิกรไทยและธนาคารออมสินเจอปัญหาการถูกโจรกรรมทางการเงิน ทั้งสองกรณีต่างกันที่กรณีธนาคารกสิกรไทยหัวขโมยอาศัยช่องโหว่ของการปกปิดข้อมูลของลูกค้า การปฏิบัติงานธนาคาร และการออกซิมโทรศัพท์ใหม่ของผู้ให้บริการโทรศัพท์มือถือ โอนเงินออกจากบัญชีลูกค้า ส่วนกรณีของธนาคารออมสินโจร

ไฮเทคใช้วิธีการติดตั้งอุปกรณ์ปล่อยไวรัสเข้าเครื่องเอทีเอ็มขโมยเงินจากธนาคาร อย่างไรก็ตาม ไม่ว่าจะสร้างความเสียหายกับลูกค้าหรือกับธนาคารนั้น ก็ถือว่าเป็นอาชญากรรมทางการเงินที่น่าเป็นห่วงทั้งสิ้น เพราะมีพัฒนาการวิธีขโมยเงินที่แยบยลขึ้นเรื่อยๆ ตามเทคโนโลยีที่เปลี่ยนแปลงไป นายอนุชิต อนุชิตานุกูล รองกรรมการผู้จัดการ ธนาคารเกียรตินาคิน ที่ปรึกษาระบบการชำระเงินของกระทรวงการคลัง กล่าวว่า ในอนาคตเราจะไม่เห็นโจรเอารถปิกอัพมาลากตู้เอทีเอ็มเอาไปเจาะเพื่อขโมยเงินภายใน แต่จะเผชิญหน้ากับโจรไฮเทคที่จะจับยากขึ้นเรื่อยๆ "ขณะนี้การค้าการชำระเงินเปิดกว้างทางอินเทอร์เน็ต มีโอกาสที่จะเจอความเสี่ยงกันทุกคน แล้วแต่ใครจะเจอแจ็กพอต" นายอนุชิต กล่าวในที่สุด

(5). การเจาะระบบ (Hacking) และการบุกรุก คือ การเจาะเข้าไปสู่โปรแกรมคอมพิวเตอร์อย่างไม่ถูกต้องตามกฎหมาย หรือผิดกฎหมายนั่นเอง การเจาะระบบ คือเจาะระบบเข้าไปโดยไม่ได้รับความยินยอมจากเจ้าของเครื่องคอมพิวเตอร์ ในหนังสือของ Jame A. O'Brien (2008) ได้อธิบายความหมายของการเจาะระบบ (Hacking) เอาไว้ว่า การเจาะระบบในระบบคอมพิวเตอร์คือการเข้าไปครอบงำการใช้เครื่องคอมพิวเตอร์ หรือผู้ที่ไม่มีสิทธิ์เข้าไปใช้เครือข่ายคอมพิวเตอร์ นักเจาะระบบ (Hacker) ในที่นี้เป็นแฮกเกอร์หมวกดำ (Black Hat Hacker) เป็นลักษณะการก่อการร้ายบนโลกไซเบอร์ หรือผ่านเครือข่ายอินเทอร์เน็ต ส่วนใหญ่เป็นการเจาะระบบเพื่อให้บรรลุเป้าหมายไม่ว่าจะเป็นทางด้านการเงิน การเมืองหรือทางสังคม เช่น การเจาะระบบขององค์กรนาโต้ ด้วยการส่งอีเมลที่มุ่งร้ายไปยังคอมพิวเตอร์เครือข่ายขององค์กรนาโต้ โดยกลุ่มผู้ก่อการร้ายที่ไม่เห็นด้วยกับการทิ้งระเบิดของนาโต้ นอกจากนี้ ยังรวมไปถึงการโจมตีเพื่อขู่เข็ญ หรือบีบบังคับรัฐบาล เพื่อวัตถุประสงค์ทางการเมืองและสังคม หรืออีกกรณีหนึ่ง เหตุการณ์เกิดขึ้นเมื่อปี ค.ศ. 2010 ที่ผู้ก่อการร้ายที่ใช้ชื่อว่า "นิรนาม" ใช้ DDoS โจมตีบริษัท มาสเตอร์การ์ด เพพาล ซิตี้แบงค์ และวีซ่า เป็นต้น ส่วนแฮกเกอร์อีกประเภทหนึ่ง คือ แฮกเกอร์หมวกขาว (White Hat Hacker) แฮกเกอร์ประเภทนี้มีคุณธรรม แต่มีความเชี่ยวชาญด้านการเจาะระบบ ทำงานให้องค์กรและบริษัทเพื่อรับมือกับแฮกเกอร์หมวกดำนั่นเอง ส่วนการบุกรุก คือ การใช้ความพยายามบุกรุกเข้าสู่ระบบคอมพิวเตอร์ที่เขามีมาตรการป้องกันความปลอดภัยเอาไว้ การบุกรุกส่วนใหญ่เป็นเรื่องการเจตนาร้าย เพื่อเข้าไปกระทำการอย่างใดอย่างหนึ่ง เช่น บุกรุกเข้าไปทำลายข้อมูล ลบ แก้ไข เปลี่ยนแปลงข้อมูล เพื่อผลประโยชน์ของตนเอง หรือเพื่อให้เกิดความได้เปรียบทางการแข่งขันธุรกิจ

(6). การโจมตีด้วยหนอน ม้าโทรจัน และไวรัส รวมถึงมัลแวร์ด้วย การโจมตีส่วนใหญ่เป็นการมุ่งร้าย เจตนาเพื่อสร้างความเสียหาย หรือผลประโยชน์ทางด้านการเงินเป็นหลัก เพราะว่าปัจจุบัน อินเทอร์เน็ตนับว่าเป็นขุมทรัพย์อันมหาศาล ที่เหล่าอาชญากรทั่วโลก มุ่งมาแสวงหาผลประโยชน์ โดยเฉพาะสถาบันทางด้านการเงิน และธนาคาร ตกเป็นเป้าหมายอันดับต้นๆ โดยมีการรายงานข่าวจากหนังสือพิมพ์ไทยรัฐ ฉบับพิมพ์ (2559) เมื่อวันที่ 28 สิงหาคม พ.ศ.2559 รายงานว่า **รู้ตัว 9 โจร! แก๊งฉก 12 ล้านออมสิน "ชาติชาย พยุหนาวีชัย"** ผอ.แบงก์ออมสินเผย บริษัทเอ็นซีอาร์ฯ ผู้ผลิตตู้เอทีเอ็มยอมรับซอฟต์แวร์ที่ใช้ในตู้เอทีเอ็มที่ถูกไวรัสเป็นรุ่นเก่า ถูกเจาะข้อมูลไปจากตู้เอทีเอ็มที่ประเทศมาเลเซีย เร่งส่งซอฟต์แวร์ตัวใหม่มาติดตั้งแล้ว คาดว่าต้องใช้เวลาประมาณ 2-3 อาทิตย์ ด้าน "ปัญญา มาเม่น" ลุยตรวจตู้เอทีเอ็มที่ถูกก่อเหตุทั้งในกรุงเทพฯ และ จ.สุราษฎร์ธานี ล่ารถต้องสงสัย 3 คันที่คนร้ายเช่าใช้ตระเวนกดเงินสด พบภาพคนร้ายมีทั้งหมด 9 คน เชื่อมีคนไทยร่วมด้วย และยังไม่พบว่ามีธนาคารอื่นถูกก่อเหตุ โดยแก๊งดังกล่าว กรณีธนาคารออมสินตรวจสอบพบว่า ถูกคนร้ายปล่อยโปรแกรมมัลแวร์ หรือโปรแกรมประสงค์ร้าย โจมตีเครื่องเอทีเอ็มของธนาคารเฉพาะยี่ห้อเอ็นซีอาร์ (NCR) ที่ตั้งอยู่นอกสถานที่ ทั้งในกรุงเทพฯ และในพื้นที่ภาคใต้ ทำให้ธนาคารสูญเงินไปทั้งสิ้น 12.29 ล้านบาท จึงระงับการใช้งานตู้เอทีเอ็มยี่ห้อดังกล่าวไว้ก่อนเพื่อตรวจสอบ และเข้าแจ้งความร้องทุกข์ตำรวจตรวจสอบพบว่าแก๊งคนร้ายน่าจะเป็นแก๊งแฮกเกอร์ชาวยุโรปตะวันออก มีภาพหลักฐานจากตู้เอทีเอ็มขณะกดเงินชัดเจน ทางการสืบสวนเชื่อว่า คนร้ายน่าจะเกี่ยวข้องกับแก๊งแฮกเกอร์ที่เคยก่อเหตุที่ประเทศไต้หวัน เชื่อว่ากลุ่มคนร้ายบางส่วนน่าจะหลบหนีออกจากประเทศไปแล้ว แต่บางส่วนน่าจะยังกบดานอยู่ในประเทศไทย

(7). การละเมิดทรัพย์สินทางปัญญา (Intellectual Property) การละเมิดทรัพย์สินทางปัญญา หมายถึง การคัดลอก หรือละเมิดทรัพย์สินทางปัญญาของบุคคลอื่น ที่ตนเองไม่ได้สร้างสรรค์ขึ้นมา ไม่ว่าจะเป็นบทความ หนังสือ เพลง ภาพยนตร์ วรรณกรรม ภาพถ่าย วิดีโอ โลโก้ เครื่องหมายทางการค้า (Trademark) หรืองานเขียนในลักษณะอื่นๆ รวมไปถึงซอฟต์แวร์คอมพิวเตอร์ด้วย การละเมิดทรัพย์สินทางปัญญาก่อให้เกิดความเสียหายต่อระบบเศรษฐกิจเป็นอย่างมากและเสียภาพลักษณ์ของประเทศด้วย การละเมิดทรัพย์สินทางปัญญา มีความผิดตาม พ.ร.บ.ลิขสิทธิ์ พ.ศ.2537 โดย มาตรา 27 ความว่า การกระทำอย่างใดอย่างหนึ่งแก่งานอันมีลิขสิทธิ์ตามพระราชบัญญัตินี้ โดยไม่ได้รับอนุญาตตามมาตรา 15 (5) ให้ถือว่าเป็นการละเมิดลิขสิทธิ์ ถ้าได้กระทำดังต่อไปนี้ (1) ทำซ้ำหรือดัดแปลง, (2) เผยแพร่ต่อสาธารณชน ส่วนมาตรา 30 ความว่า การกระทำอย่างใดอย่างหนึ่งแก่โปรแกรมคอมพิวเตอร์อันมีลิขสิทธิ์ตามพระราชบัญญัตินี้โดยไม่ได้รับอนุญาตตามมาตรา 15 (5) ให้ถือว่าเป็นการละเมิดลิขสิทธิ์ ถ้าได้กระทำดังต่อไปนี้ (1) ทำซ้ำหรือดัดแปลง, (2) เผยแพร่ต่อสาธารณชน, (3) ให้เช่าต้นฉบับหรือสำเนางานดังกล่าว โดยในมาตรา 69 ระบุความว่า ผู้ใดกระทำการละเมิดลิขสิทธิ์ ตามมาตรา 27 มาตรา มาตรา 30 หรือมาตรา 52 ต้องระวางโทษปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

(8). การส่งไปรษณีย์อิเล็กทรอนิกส์ ข้อความไร้สาระ หรือสแปมมิ่ง (Spamming) เพื่อรบกวนและสร้างความรำคาญเดือดร้อนให้กับผู้อื่น การส่งสแปมมิ่ง คือ การส่งจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ไม่ได้ร้องขอ หรือที่ไม่ได้รับเชิญเป็นจำนวนมาก ผ่านทางระบบอิเล็กทรอนิกส์ เช่น ส่งผ่านทางอีเมลที่ไม่ถูกต้อง ทำให้ผู้รับเกิดความรำคาญไม่พอใจ สแปมมิ่งที่พบเห็นกันได้บ่อยคือการส่งผ่านทางอีเมล ซึ่งเป็นการโฆษณาขายสินค้า หรือชวนเชื่อ เป็นอีเมลที่เราไม่มีความต้องการ ซึ่งมาจากทั่วทุกมุมโลก โดยที่เราไม่สามารถรู้ได้เลยว่า ผู้ที่ส่งมานั้นเป็นใคร จุดประสงค์หลักของพวกเขาคือ ต้องการโฆษณาสินค้า และการบริการต่างๆ ซึ่งนับได้ว่าเป็นอีเมลประเภทหนึ่งของอีเมลขยะ สแปมมิ่งนี้ ซึ่งนอกจากจะทำให้ผู้รับเกิดความรำคาญแล้ว บุคคลผู้ที่นิยมส่งอีเมลหรือข้อความเหล่านี้ ก็เพราะเป็นทฤษฎีหนึ่งของการทำการตลาด และมีต้นทุนที่ต่ำมาก หรือบางครั้งอาจมาจากเว็บไซต์ลามกอนาจาร หรือมาจากการที่เราเคยไปสมัครและตอบแบบสอบถามเอาไว้เกี่ยวกับการวิจัยสินค้าและถูกบริษัทที่ถูกต้องตามกฎหมายนำเอาไปใช้ประโยชน์ ข้อเสียของสแปมมิ่งทำให้ประสิทธิภาพการส่งจดหมายอิเล็กทรอนิกส์ หรือการส่งข้อมูลอื่นๆ บนอินเทอร์เน็ตช้าลงด้วย หรือบางครั้งอาจทำให้กล่องจดหมายเต็ม จดหมายถูกตีกลับ ทำให้ผู้รับไม่ทราบข้อมูลข่าวสาร สแปมมิ่งในรูปแบบอื่นๆ ก็มี นอกจากอีเมลสแปมมิ่ง คือ แมสเซนเจอร์สแปม นิวส์กรุ๊ปสแปม บล็อกสแปม เอสเอ็มเอสสแปม นอกจากนี้ ปัจจุบันยังมีเฟซบุ๊กสแปมอีกด้วย ปัจจุบันบริษัทผู้ให้บริการอีเมลต่างๆ ส่วนใหญ่มักจะมีเครื่องกรองไปรษณีย์อิเล็กทรอนิกส์ ที่เรียกกันว่า ตัวเครื่องกรองสแปม (Spamming Filter) และซอฟต์แวร์กรองอีเมล ซึ่งสามารถตรวจจับไปรษณีย์อิเล็กทรอนิกส์ได้ถึง 95% เช่น Gmail เป็นต้น หรืออาจจะไปสมัครในเว็บไซต์ที่มีเครื่องมือกรองสแปมมิ่ง เช่น เว็บไซต์ emaillias.com และ sneaknail.com

(9) การสมรู้ร่วมคิดในการใช้อุปกรณ์คอมพิวเตอร์ และเครือข่าย การสมรู้ร่วมคิดส่วนใหญ่จะเป็นพนักงานในองค์กรสมรู้ร่วมคิดกับบุคลภายนอก เพราะว่าพนักงานภายในจะรู้ข้อมูลระบบการป้องกัน และรักษาความมั่นคงปลอดภัยขององค์กร หรือบางครั้งอาจเป็นพนักงานที่ถูกให้ออก และเกิดความโกรธแค้นองค์กร แล้วกลับมาแก้แค้นองค์กร เหตุการณ์เหล่านี้เกิดขึ้นบ่อยครั้ง โดยเฉพาะสถาบันทางด้านการเงิน และธนาคาร

(10).การโกงการประมูล, การไม่ส่งสินค้าให้ลูกค้าตามใบสั่งซื้อ การโกงการประมูล ส่วนใหญ่มักจะเป็นเว็บไซต์ที่มีการประมูลสินค้าอิเล็กทรอนิกส์ เช่น ebay.com หรือ pramool.com หรือแม้กระทั่งการประมูลสินค้ากับทางหน่วยงานราชการที่เรียกกันว่า e-auction เพราะก่อนจะมีการประมูลกันจริงผ่านระบบคอมพิวเตอร์แล้ว อาจจะมีการประมูลกันมาก่อนหน้านี้แล้วที่เราเข้าใจกันโดยทั่วไปว่าเป็นการ "ฮั้วประมูล หรือฮั้วราคา" กันนั่นเอง สำหรับตัวอย่างการโกงการประมูลในเว็บไซต์ e-bay.com นั้น ซึ่งเขียนโดย KARL THOMAS และแปลโดย WORAPON H. (2017). เรื่อง **"7 กลโกงบน e-Bay และวิธีรับมือ"** ความว่า ทาง Welivesecurity และ Blog ESET จึงนำกลโกงของมิจฉาชีพ

มาให้ทุกคนได้รู้ และตามทันพวกเขา **กลโกง eBay 1: รูปภาพราคาแพง** ถือเป็นเหตุการณ์ที่ซื้อควงการซื้อขายออนไลน์ก็ว่าได้ ในประเทศอังกฤษมีคนเปิดประมูลสินค้าที่กำลังเป็นที่ต้องการอย่าง Xbox One และ MacBook ซึ่งมีผู้ให้ความสนใจจำนวนมาก แต่พอถึงเวลากลับเป็นภาพถ่ายของสินค้า และผู้ซื้อก็ไม่สามารถเถียงอะไรได้เลยเมื่อผู้ขายบอกว่าเขาเขียนทุกอย่างลงไปใน Description ตั้งแต่แรกแล้ว **วิธีหลีกเลี่ยง:** อ่านรายละเอียดสินค้าอย่างละเอียดเสมอ ไม่ว่าคุณจะซื้ออะไรก็ตาม และมีสติเสมอเมื่อคุณกำลังได้รับข้อเสนอที่สุดแสนพิเศษ เพราะอะไรที่มันดีเกินกว่าจะเป็นจริง อาจไม่จริงก็ได้ และตรวจสอบประวัติของผู้ขายว่าเคยขายสินค้าอะไรมาบ้าง เพราะแอคเค้าท์ที่ตั้งขึ้นมาอาจสร้างมาเพื่อตั้งแคมเปญจน์ปลอมก็เป็นได้ **ส่วนกลโกง eBay 2: บัญชี PayPal ปลอม** กลโกงนี้อาจเกิดขึ้นเมื่อคุณอยู่ในฐานะผู้ขายสินค้าบน eBay เริ่มต้นจากผู้ซื้อ (ต้องสงสัย) จะทำการประมูลสินค้าของคุณ และส่งอีเมล์เข้ามาหาคุณว่า คุณได้รับยอดเงินจากการขายสินค้าบนบัญชี PayPal แต่จริงๆ แล้วผู้ขายกลับไม่ได้รับเงินจำนวนนั้น **วิธีหลีกเลี่ยง:** ตรวจสอบเงินที่เข้าในบัญชี PayPal ทุกครั้งหลังได้รับอีเมล์ เพราะอาจเป็นของมิจฉาชีพส่งมาก็ได้ และอย่าคลิกลิงก์ในอีเมล์เด็ดขาด ให้ใช้วิธีเข้าผ่านเว็บไซต์แทน และตรวจสอบประวัติของผู้ซื้อด้วย เพราะหลายครั้งเราอาจพบที่อยู่ที่ไม่มีอยู่จริง

ส่วน **การไม่ส่งสินค้าให้ลูกค้าตามใบสั่งซื้อ** นั้น เราจะได้ยินข่าวอยู่บ่อยครั้ง ไม่ว่าจะเป็นการสั่งซื้อสินค้าผ่านระบบออนไลน์ เช่น lazada, shoppee และ Facebook แล้วไม่ส่งสินค้าให้กับลูกค้า หรือมีการส่ง แต่ส่งสินค้าไม่ตรงกับที่ลูกค้าสั่งซื้อ เป็นต้น

(11).การปลอมแปลงบัตรเครดิตและการหักเงินในบัญชี ในประเด็นนี้หมายความว่า โจรไซเบอร์ใช้วิธีการปลอมแปลงบัตรเครดิต สมาร์ทการ์ด บัตรเอทีเอ็ม ด้วยวิธีการต่างๆ เช่น การใช้เครื่อง ATM Skimmer ส่วนหนึ่งเกิดจากแก๊งปลอมบัตรเครดิตข้ามชาติ เช่น ตัวกอย่าง กลโกง (2016). ได้รายงานข่าวในเว็บ https://moneyhub.in.th/ เรื่อง **"มาอีกแล้ว ! แก๊งสกิมเมอร์ปลอมบัตรเครดิตข้ามชาติ"** ความว่า มีแก๊งปลอมแปลงบัตรเครดิตเป็นแก๊งชาวไนจีเรีย 2 คนที่ตำรวจได้ทราบข่าวมาว่ามีแก๊งที่ใช้บัตรเอทีเอ็มปลอมไปกดเงินสดจากตู้เอทีเอ็มในย่านนานา ถนนสุขุมวิท เมื่อนำกำลังไปตรวจสอบก็พบคนร้ายกำลังใช้บัตรเอทีเอ็มปลอมกดเงินสดอยู่ที่ตู้เอทีเอ็มหน้าธนาคารกสิกรไทย สาขานานาเหนือ จึงจับกุมและนำกำลังเข้าตรวจค้นโรงแรมที่พักในย่านสุขุมวิท พบของกลางเป็นบัตรเอทีเอ็มปลอมจำนวนถึง 199 ใบ เงินสดอีก 34,200 บาท ผู้ต้องหาทั้ง 2 คนที่เป็นชาวไนจีเรียทั้งคู่รับสารภาพว่าได้นำบัตรเอทีเอ็มปลอมจากประเทศไนจีเรียเพื่อมากดเงินสดที่ตู้เอทีเอ็มในเมืองไทย

(12). การหลอกลวงทางอินเทอร์เน็ต หรือฟิชชิง (Phishing) คือ การที่อาชญากรไซเบอร์ ใช้วิธีการส่งอีเมลตลบตะแลงไป เพื่อให้ผู้ใช้งานคอมพิวเตอร์เปิดเผยข้อมูลส่วนบุคคลออกมา ไม่ว่าจะเป็น หมายเลขบัตรเครดิต บัตรเอทีเอ็ม บัตรประจำตัวประชาชน ใบขับขี่ ที่อยู่และหมายเลขโทรศัพท์ หมายเลข PIN Code รวมถึงหมายเลขบัญชีธนาคาร เป็นต้น วิธีการทำ **ฟิชชิ่ง (Phishing) คือการตกปลา** คล้ายกับวิธีการใช้เหยื่อล่อปลาให้มาติดเบ็ด การหลอกลวงทางอินเทอร์เน็ต ในปัจจุบันมีหลากหลายวิธี เช่น การส่งอีเมลแจ้งว่า จากการที่ทางเราได้สุ่มคัดเลือกอีเมลของบุคคลผู้โชคดี ปรากฏว่า อีเมลของคุณได้รับการจับฉลาก หรือได้รับการคัดเลือก ให้เป็นผู้ที่โชคดีได้รับรางวัล จำนวน 1 ล้านดอลล่าร์ หลังจากนั้น ก็ทำการส่งอีเมลไปหลายหมื่นอีเมล และในจำนวนนั้นอาจมีคนหลงชื่อ จำนวน 1-3 คน เขาก็ประสบความสำเร็จแล้ว เหมือนกับการที่มีปลาเข้ามาติดเบ็ดนั่นเอง จดหมายนี้ที่เคยโด่งดังมาก เกี่ยวกับเรื่องนี้ คือ จดหมายจากไนจีเรีย นอกเหนือจากนั้นก็ยังมีอีกหลากหลายวิธีการ เช่น การหลอกลวงผ่านทางเฟซบุ๊ก โดยทำโปรไฟล์ปลอม หลอกสาวไทยแต่งงาน หรือแม้กระทั่งเรื่อง การหลอกให้ลงทุนเกี่ยวกับแชร์ เป็นต้น

บทสรุป

ดังนั้น จะเห็นได้ว่า อาชญากรรมไซเบอร์: ภัยคุกคามรูปแบบใหม่ในบริบทประเทศไทย 4.0 ที่เกิดขึ้นนั้น อาจเกิดจากปัจจัยหลายสาเหตุ คือ (1). สิ่งแวดล้อมทางคอมพิวเตอร์มีความซับซ้อนมากขึ้น (2). ผู้ใช้งานคอมพิวเตอร์มีความคาดหวังต่อการใช้คอมพิวเตอร์สูงมาก และ (3). การขยายตัวและการเปลี่ยนแปลงของระบบเครือข่ายคอมพิวเตอร์ ซึ่งเท่ากับเป็นความเสี่ยงใหม่ นอกจากนี้ยังมีอาชญากรรมทางไซเบอร์ในรูปแบบต่างๆ ไม่ว่าจะเป็นการเจาะระบบ การแก้ไขเปลี่ยนแปลงทำลายข้อมูล การบุกรุก การฉ้อโกง และการหลอกลวงทางอินเทอร์เน็ต เป็นต้น อันเป็นภัยรูปแบบใหม่ซึ่งอยู่บนอินเทอร์เน็ต ซึ่งนับวันจะมีปริมาณเพิ่มมากขึ้นเป็นลำดับ และสร้างความเสียหายต่อระบบเศรษฐกิจของประเทศไทยเป็นอย่างมาก ใน เร็ค คอม เมนด์ (Recommended). (2563). หนังสือพิมพ์กรุงเทพธุรกิจ ได้รายงานข่าวเรื่อง "TIJ **จับมือ UNODC ปลุกปั้นไทยสู้อาชญากรรมไซเบอร์"** ความว่า การเติบโตของ **"อาชญากรรมไซเบอร์"** ที่ก้าวกระโดดไม่แพ้ความก้าวหน้าของเทคโนโลยีข้อมูลที่เก็บรวบรวมโดยกองบังคับการปราบปรามการกระทำ ความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือ บก.ปอท. พบว่าอาชญากรรมไซเบอร์มีมูลค่าความเสียหายสูงขึ้นอย่างต่อเนื่อง จาก 527 ล้านบาทเศษในปี 2561 พุ่งขึ้นเป็นกว่า 573 ล้านบาทในปี 2562 ส่วนปี 2563 แม้จะเจอผลกระทบจากโควิด-19 แต่มูลค่าความเสียหายก็ยังสูงต่อเนื่อง ข้อมูล ณ สิ้นเดือน ก.ย. ตัวเลขอยู่ที่กว่า 330 ล้านบาท จำนวนประชาชนที่เข้าร้องทุกข์ใกล้เคียงกับปี 2552 ทั้งปี นั่นก็คือมากกว่า 3,000 คดี ขณะที่รูปแบบการกระทำความผิด ทั้งแฮ็ก ขโมย และทำลายข้อมูล, หลอกขายสินค้าและบริการ รวมถึงหลอกโอนเงิน และการหมิ่นประมาทผ่านสื่อสังคมออนไลน์ มีทิศทางสูงขึ้นทุกประเภทความผิด โดยข้อมูลนี้เป็นเพียงส่วนหนึ่งที่ปรากฏสู่สาธารณะผ่านการแจ้งความร้องทุกข์กับหน่วยงานของรัฐ จึงเปรียบได้กับ **"ยอดภูเขาน้ำแข็ง"** เท่านั้น เพราะยังมีการกระทำผิดอีกจำนวนมากที่ไม่ได้ถูกส่งเข้ากระบวนการยุติธรรม จากข้อมูลดังกล่าวเหล่านี้ องค์กรภาคธุรกิจต่างๆ ต้องตระหนักรู้ และหาแนวทางป้องกันอาชญากรรมไซเบอร์เอาไว้ให้อย่างเข้มแข็ง เพราะว่า **"การป้องกันย่อมดีกว่าการมาทำการแก้ไขในภายหลัง"** อย่างแน่นอน.

เอกสารอ้างอิง

กลโกง. (2016). **มาอีกแล้ว ! แก๊งสกิมเมอร์ปลอมบัตรเครดิตข้ามชาติ** สืบค้นเมื่อวันที่ 21 ธันวาคม 2563, จาก https://moneyhub.in.th/

คาร์ล โทมัส (KARL THOMAS) และวรพล ฮ. (WORAPON H.). (2017). **7 กลโกงบน e-Bay และวิธีรับมือ** สืบค้นเมื่อวันที่ 21 ธันวาคม 2563 จาก, https://blog.eset.co.th/

ทีมข่าวการเงินโพสต์ทูเดย์, (2563). **โจรไฮเทค ภัยที่มาพร้อมธนาคารออนไลน์** สืบค้นเมื่อวันที่ 20 ธันวาคม 2563, จาก https://www.posttoday.com/

ไทยเซิร์ต, (2563). **สถิติภัยคุกคาม,** สืบค้นเมื่อวันที่ 22 ธันวาคม 2563, จาก https://www.thaicert.or.th/

หนังสือพิมพ์ไทยรัฐ. (2559). **รู้ตัว 9 โจร! แก๊งฉก 12 ล้านออมสิน หนังสือพิมพ์ไทยรัฐ ฉบับพิมพ์** ฉบับวันที่ 28 สิงหาคม พ.ศ.2559 หน้า 1 สืบค้นเมื่อวันที่ 20 ธันวาคม 2563, จาก https://www.thairath.co.th/content/704109

ธนนท์ทัส สุธริยานิติภักดี. (2563). **อาชญากรรมคอมพิวเตอร์กรณีศึกษามาตรการป้องกันการเข้าถึงข้อมูลทางอินเทอร์เน็ตโดยมิชอบ** สืบค้นเมื่อวันที่ 20 ธันวาคม 2563, จาก http://acad.vru.ac.th/acad_journal_online/journalFile/datajournaP220.pdf

พงศ์สุข หิรัญพฤกษ์. (2561). **TREND IT 2018 Live สดทันที ที่มีเรื่องกับหนุ่ยแบไต๋,** สืบค้นเมื่อวันที่ 17 ธันวาคม 2563, จาก https://kmtlcspu.com/2017/11/16/trend-it-2018/

พิมพ์ธรา พัสดุประดิษฐ์. (2563). **แนวทางการเพิ่มประสิทธิภาพในการปฏิบัติงานรักษาความปลอดภัยนักท่องเที่ยวของข้าราชการตำรวจในสังกัดกองกำกับการ 3 กองบังคับการตำรวจท่องเที่ยว 1,** วารสารคุณภาพชีวิตกับกฎหมาย, ปีที่ 16 ฉบับที่ 1, หน้า 93. สืบค้นเมื่อวันที่ 15 กุมภาพันธ์ 2564, จาก Quality of Life and Law Jour - ThaiJOso05.tci-thaijo.org

ฟอร์ไซท (Foresight). (2562). **ETDA เผย ปี 62 คนไทยใช้อินเทอร์เน็ตเพิ่มขึ้นเฉลี่ย 10 ชั่วโมง 22 นาที Gen Y ครองแชมป์ 5 ปีซ้อน,** สืบค้นเมื่อวันที่ 20 ธันวาคม 2563, จาก https://www.etda.or.th/

เร็ค คอม เมนด์ (Recommended) (2563). **TIJ จับมือ UNODC ปลุกปั้นไทยสู้อาชญากรรมไซเบอร์** สืบค้นเมื่อวันที่ 22 ธันวาคม 2563 จาก https://www.bangkokbiznews.com/

สุพล พรหมมาพันธุ์. (2562). **ปัจจัยที่มีผลกระทบต่อจริยธรรม และความมั่นคงปลอดภัยทางด้านเทคโนโลยีสารสนเทศ ในบริบทของประเทศไทย 4.0: กรณีศึกษา สถาบันอุดมศึกษาในเขตกรุงเทพมหานคร และปริมณฑล,** วารสารแพทยสารทหารอากาศ, ปีที่ 65 ฉบับที่ 3, หน้า 69-70.

George W. Reynolds. (2012). **Ethics in Information Technology,** Fourth Edition, United State, Course Technology, CENGAGE Learning.

Jame A. O'Brien. (2008). **Management Information Systems,** Eighth Edition, New York, McGraw Hill Companies Inc.