อาชญากรรมบนอินเทอร์เน็ต

พ.ต.อ.สุรัตน์ สาเรือง*

บทคัดย่อ

ภัยจากอาชญากรรมบนอินเทอร์เน็ตในสังคมไทยเพิ่มมากขึ้น ได้แก่ ภัยจากการหลอกลวงซื้อขายสินค้าออนไลน์ การหลอกลวงให้โอนเงินในรูปแบบต่างๆ การโจรกรรมข้อมูล การเจาะระบบและการโจมตีระบบคอมพิวเตอร์ มัลแวร์เรียกค่าไถ่ข้อมูล ด้วยเหตุนี้ ผู้วิจัยจึงได้ทำการวิจัยโดยมีวัตถุประสงค์เพื่อ (1) ศึกษาแผนประทุษกรรมของคนร้ายคดีอาชญากรรมบนอินเทอร์เน็ต (2) ศึกษาแนวทางการสืบสวนจับกุมคนร้ายคดีอาชญากรรมบนอินเทอร์เน็ต (3) ศึกษาแนวทางการระวังป้องกันอาชญากรรมบนอินเทอร์เน็ต การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยการศึกษาค้นคว้าเอกสาร และการสัมภาษณ์เจ้าหน้าที่ตำรวจ พนักงานสอบสวน เจ้าหน้าที่กรมสอบสวนคดี ที่ทำสำนวนคดีเกี่ยวกับอาชญากรรมคอมพิวเตอร์ จำนวน 25 คน

ผลการศึกษาพบว่า (1) แผนประทุษกรรมคดีอาชญากรรมบนอินเทอร์เน็ต คนร้ายมีทักษะความชำนาญทางคอมพิวเตอร์ ทักษะการเรียนรู้จุดอ่อนของเหยื่อทำให้เหยื่อหลงเชื่อและให้ข้อมูล ขั้นตอนการหลอกลวงเพื่อเอาข้อมูลส่วนตัว เรียกว่า Social Engineering (2) แนวทางการสืบสวนคดีอาชญากรรมบนอินเทอร์เน็ต ประสบความสำเร็จเนื่องจากได้ข้อมูลการเชื่อมต่ออินเทอร์เน็ต ข้อมูลการเชื่อมต่อสื่อสารโทรศัพท์มือถือ ข้อมูลการโอนเงิน ข้อมูล

* คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

จากกล้องวงจรปิด โดยได้รับความร่วมมือการสืบสวนทั้งระหว่างหน่วยงานและระหว่างประเทศ การตรวจพิสูจน์วัตถุพยานทางดิจิทัล ตามหลักการห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of custody) (3) แนวทางการระวังป้องกันอาชญากรรมบนอินเทอร์เน็ต ได้แก่ การสื่อสารเพื่อสร้างความเข้าใจให้กับประชาชน การสร้างความตระหนักถึงภัยที่อาจเกิดขึ้น การเฝ้าระวังการโจมตีระบบคอมพิวเตอร์ การจัดทำแผนบริหารการจัดการความเสี่ยงให้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยีสารสนเทศ การเตรียมความพร้อมรับสถานการณ์การโจมตีให้กับบุคลากรทั้งภาครัฐและเอกชน

คำสำคัญ: อาชญากรรมคอมพิวเตอร์ อินเทอร์เน็ต แผนประทุษกรรม

Crimes on the Internet

Pol.Col.Surat Saruang*

Abstract

Cybercrime is a growing problem. Also, it is a relatively new field of criminology. This study focuses on cybercrime in the unique online environment of Thailand, including online shopping scams, money transfer scams, data thefts, and hacking and malware threats. Objectives of this study are: (1) to describe modus operandi of different types of cybercrimes in order to understand those cyber threats, (2) to study the guidelines for investigating the cybercriminal cases, and (3) to study how to protect people against social media scams. This qualitative research was conducted by interviewing twenty-five police officers and officers from the Department of Special Investigation.

The results show that: (1) modus operandi of different types of cybercrimes are mostly conducted by offenders who have computer skills and understand weakness of the victims to lure unsuspecting victims into sending them their confidential data, This process is

* Faculty of Forensic Science, Royal Police Cadet Academy

known as “Social Engineering”, (2) Investigating computer crimes is successful because national and international cooperation and the providing of digital evidences, and (3) The guidelines to prevent cybercrime can help people to be aware of those cyber threats.

อาชญากรรมบนอินเทอร์เน็ต

พ.ต.อ.สุรัตน์ สาเรือง

บทนำ

เมื่อสังคมไทยเข้าสู่ในยุคระบบเศรษฐกิจและสังคมดิจิทัล เทคโนโลยีดิจิทัลเข้ามาเป็นส่วนหนึ่งในการดำเนินชีวิตประจำวันทั้งในเรื่องส่วนตัวและการทำงาน การเชื่อมต่อด้วยอินเทอร์เน็ตมีอิทธิพลอย่างมากในการดำรงชีวิตประจำวัน มีการนำเทคโนโลยีสารสนเทศมาประยุกต์ใช้ให้เข้ากับกิจกรรมทางเศรษฐกิจ เช่น การขายสินค้าออนไลน์ การใช้บริการธนาคารออนไลน์ การสนทนาผ่านทางสื่อสังคมออนไลน์ ในขณะเดียวกันปรากฏการณ์ของอาชญากรรมคอมพิวเตอร์ที่เกิดขึ้น มีทั้งการเจาะระบบคอมพิวเตอร์ การโจรกรรมข้อมูล การพนันออนไลน์ การล่อลวง การค้าประเวณี การขายยาสลบ การเผยแพร่สื่อลามกเด็ก การฉ้อโกง การหลอกลวงด้วยการโฆษณาขายบนอินเทอร์เน็ต การหลอกลวงทางอินเทอร์เน็ตเพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมล หรือการส่งข้อความผ่านสื่อโซเชียลมีเดียแนวโน้มเพิ่มมากขึ้น และอาชญากรมีความรู้ของการประกอบธุรกิจ เทคนิคทางคอมพิวเตอร์สมัยใหม่เพิ่มความสลับซับซ้อนมาผสมผสานกับการกระทำความผิดเพิ่มมากขึ้น ซึ่งยากต่อการสืบสวนและการบังคับใช้กฎหมาย

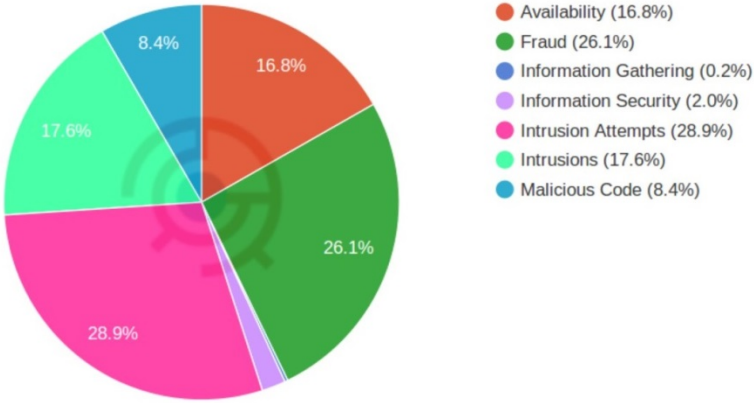
---

* คณะนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

จากสถิติอาชญากรรมคอมพิวเตอร์และภัยคุกคามบนอินเทอร์เน็ตที่เกิดขึ้นในประเทศไทย พ.ศ.2560 พบการแจ้งเหตุภัยคุกคาม ทั้งสิ้น 3,237 เรื่อง

ตารางที่ 1 ตารางแสดงสถิติภัยคุกคามบนอินเทอร์เน็ตในประเทศไทย พ.ศ. 2560

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
Abusive content	0	0	0	0	0	0	0	0	0	0	0	0	**0**
Availability	100	218	212	0	0	9	1	0	0	0	0	0	**540**
Fraud	60	60	71	55	60	70	103	81	80	50	63	88	**841**
Information gathering	1	4	3	0	0	0	0	0	0	0	0	0	**8**
Information security	0	1	19	0	0	0	0	14	15	7	4	8	**68**
Intrusion Attempts	85	65	89	106	84	88	74	62	52	78	79	77	**939**
Intrusions	157	35	84	47	18	42	40	29	19	23	51	25	**570**
Malicious code	25	31	29	26	32	29	14	19	6	20	7	33	**271**
Other	0	0	0	0	0	0	0	0	0	0	0	0	**0**
รวม	428	414	507	234	194	238	232	205	172	178	204	231	3,237



ภาพที่ 1 แสดงร้อยละการแจ้งเหตุภัยคุกคามบนอินเทอร์เน็ตในประเทศไทย พ.ศ.2560

สถิติภัยคุกคามบนอินเทอร์เน็ตในประเทศไทย พ.ศ.2560 (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, 2560) ภัยคุกคามอันดับแรก ประมาณร้อยละ 28.9 (จำนวน 939 เรื่อง) เป็นภัยคุกคามที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusion Attempts) ภัยคุกคามอันดับสอง ประมาณ ร้อยละ 26.1 (จำนวน 841 เรื่อง) เป็นภัยคุกคามที่เกิดจากการฉ้อโกงหรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) และ ภัยคุกคามอันดับสาม ประมาณ ร้อยละ 17.6 (จำนวน 570 เรื่อง) เป็นภัยคุกคามที่เกิดกับระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต (Intrusions) ข้อมูลดังภาพที่ 1 และ ตารางที่ 1

ความเสียหายทางทรัพย์สินคดีอาชญากรรมคอมพิวเตอร์จากข้อมูลการแถลงผลงานสำนักงานตำรวจแห่งชาติ ประจำปีงบประมาณ 2560 (1 ต.ค.2560 – 28 ก.ย.2561) (กองบัญชาการตำรวจท่องเที่ยว,2561)

- ความผิดเกี่ยวกับการฉ้อโกงประชาชนผ่านสื่อสังคมออนไลน์ จับกุมผู้ต้องหา 120 ราย มีประชาชนตกเป็นเหยื่อกว่า 5,000 ราย มูลค่าความเสียหายกว่า 3,000 ล้านบาท
- คดีโรแมนซ์ สแกม (Romance scam) ความเสียหายคิดเป็นมูลค่า 85,529,454 บาท โดยยึดและอายัดทรัพย์สินคืนเงินให้แก่ผู้เสียหาย จำนวน 9 ราย คิดเป็นมูลค่า 2,085,000 บาท
- คดีแก๊งคอลเซ็นเตอร์ รับแจ้งความ 503 คดี ความเสียหายคิดเป็นมูลค่า 259,294,632 บาท
- คดีการพนันออนไลน์ มีการร้องทุกข์ดำเนินคดี 32 คดี กับผู้เปิดบัญชีเงินฝาก 59 ราย ที่รับโอนเงินการพนัน แล้วขยายผลไปยังกลุ่มนายทุน โดยอายัดบัญชีเงินฝาก 122 บัญชี คิดเป็นมูลค่า 20 ล้านบาท

จากข้อมูลเชิงสถิติอาชญากรรมคอมพิวเตอร์และมูลค่าความเสียหายมหาศาลที่เกิดในประเทศไทย จึงนำมาสู่การศึกษาวิจัยเรื่องอาชญากรรม

บนอินเทอร์เน็ตในประเทศไทย เพื่อศึกษาแผนประทุษกรรมของคนร้ายคดีอาชญากรรมบนอินเทอร์เน็ต แนวทางการสืบสวนจับกุมคนร้ายคดีอาชญากรรมบนอินเทอร์เน็ต และแนวทางการป้องกันอาชญากรรมบนอินเตอร์เน็ต เพื่อนำมาใช้ในการเรียนการสอนของสถาบันวิชาการตำรวจและการบริการวิชาการแก่สังคม

วัตถุประสงค์ของการวิจัย

1) เพื่อศึกษาแผนประทุษกรรมของคนร้ายคดีอาชญากรรมบนอินเทอร์เน็ต

2) เพื่อศึกษาแนวทางการสืบสวนจับกุมคนร้ายคดีอาชญากรรมบนอินเทอร์เน็ต

3) เพื่อศึกษาแนวทางการระวังป้องกันอาชญากรรมบนอินเทอร์เน็ต

ขอบเขตของการวิจัย

1) เน้นการสัมภาษณ์พนักงานสอบสวน เจ้าหน้าที่สืบสวน จากสำนักงานตำรวจแห่งชาติและกรมสอบสวนคดีพิเศษ ประกอบกับการศึกษาค้นคว้าเอกสาร สำนวนการสอบสวน รายงานการสืบสวน สถิติอาชญากรรมที่เกี่ยวข้อง เพื่อทำให้ทราบถึงแผนประทุษกรรมของคนร้ายคดีอาชญากรรมบนอินเทอร์เน็ตนำไปเป็นแนวคิด วิธีการ การสืบสวนจับกุมคนร้าย

2) ข้อมูลจากการสัมภาษณ์พนักงานสอบสวน ประกอบด้วยการสอบปากคำผู้เสียหาย คำให้การของเจ้าหน้าที่สืบสวน คำให้การผู้ต้องหา สามารถนำมาวิเคราะห์รูปแบบเพื่อเป็นแนวทางการระวังป้องกันอาชญากรรมบนอินเทอร์เน็ต

วิธีดำเนินการวิจัย

การวิจัยนี้เป็นการวิจัยเชิงคุณภาพ โดยการสัมภาษณ์เจ้าหน้าที่ตำรวจ พนักงานสอบสวน เจ้าหน้าที่กรมสอบสวนคดี และผู้เชี่ยวชาญคดีอาชญากรรมคอมพิวเตอร์ จำนวน 25 คน และการรวบรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลที่ได้รับการยอมรับและเชื่อถือได้ ในรูปแบบของตาราง แผนภาพ คำอธิบาย ทั้งเอกสารวิชาการ รายงานการวิจัยที่เกี่ยวข้องอาชญากรรมคอมพิวเตอร์ เพื่อวิเคราะห์แผนประทุษกรรมคดีอาชญากรรมบนอินเทอร์เน็ตที่เกิดขึ้นในประเทศไทย แนวทางการสืบสวนคดีอาชญากรรมบนอินเทอร์เน็ต แนวทางการระวังป้องกันอาชญากรรมบนอินเทอร์เน็ต

ผลการศึกษาวิจัย

แผนประทุษกรรม คือ การกระทำที่คนร้ายได้กระทำไปเพื่อให้การประกอบอาชญากรรมนั้นสำเร็จ จัดเป็นพฤติกรรมการเรียนรู้ที่คนร้ายพัฒนาเปลี่ยนแปลงได้ตามทักษะความชำนาญตลอดจนประสบการณ์ที่เพิ่มขึ้น รวมถึงความมั่นใจจากการที่ก่ออาชญากรรมสำเร็จมาแล้ว ในการตัดสินว่าสิ่งใดเป็นแผนประทุษกรรมของคนร้ายให้ดูจากกระบวนการในการประเมินวิเคราะห์สถานที่เกิดเหตุเป็นหลักว่า สิ่งใดเป็นสิ่งที่กระทำไปเพื่อให้ประสบผลสำเร็จในการก่ออาชญากรรม การปกปิดหลักฐานที่บ่งชี้ว่าตนเองเป็นคนร้ายและการทำให้ประสบผลสำเร็จในการหลบหนี กระทำไปเพื่อตอบสนองต่ออารมณ์ความรู้สึกหรือความต้องการด้านจิตใจของคนร้าย เพราะฉะนั้นการพยายามทำความเข้าใจในแผนประทุษกรรมจะทำให้สามารถเชื่อมโยงในการสืบสวนคดีต่างๆ ได้เป็นอย่างดี (สฤษดิ์ สืบพงษ์ศิริ, 2560)

ความหมายของอาชญากรรมคอมพิวเตอร์ในภาษาอังกฤษมีคำศัพท์ที่ใช้เรียกหลายคำ เช่น Computer crime, Cyber crime, E-crime, Online crime, High-tech crime และ Computer abuse คำเหล่านี้มีความหมายในทำนองเดียวกันและสามารถใช้แทนกันได้

อาชญากรรมคอมพิวเตอร์ หมายถึง การกระทำที่ผิดกฎหมายโดยใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือ หรือการกระทำที่ผิดกฎหมายที่ก่อให้เกิดความเสียหายแก่ระบบคอมพิวเตอร์ซึ่งคอมพิวเตอร์อาจเป็นวัตถุแห่งการกระทำความผิด(the target of crime) หรือเป็นเครื่องมือที่ใช้ในการกระทำความผิด(a tool in the commission of crime) หรือคอมพิวเตอร์อาจมีส่วนเกี่ยวข้องกับการกระทำความผิด (Chris Kim ,2012)

อาชญากรรมบนอินเทอร์เน็ตในปัจจุบันมีมากมายหลายรูปแบบ ได้แก่ มัลแวร์เรียกค่าไถ่ (Ransomware), การโจมตีเว็บไซต์ (Web Attacks), การหลอกลวงแบบฟิชชิ่ง (Phishing),การเจาะระบบ (Hack), การก่อการร้ายทางไซเบอร์ (Cyberterrorist), การโจมตีระบบ (Attack),โปรแกรมที่ไม่พึงประสงค์(Malware), การเจาะรหัสผ่าน (Password Cracking), การดักรับข้อมูล (Sniffers), การโจมตีแบบ Distributed Denial of Service และ คนร้ายใช้เทคนิคการเรียนรู้จุดอ่อนของเหยื่อทำให้เหยื่อหลงเชื่อและให้ข้อมูลขั้นตอนการหลอกลวงเพื่อเอาข้อมูลส่วนตัว จะเรียกว่า Social Engineering

พ.ต.อ.สัญญา เนียมประดิษฐ์ ผู้กำกับการ กองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ระบุว่าในช่วงปี 2560 อาชญากรรมทางไซเบอร์ในประเทศไทย ที่พบมาก ได้แก่ 1) การหมิ่นพระบรมเดชานุภาพ 2) การหมิ่นประมาทผู้อื่น 3) การเจาะระบบ 4) การนำเข้าสู่ระบบซึ่งข้อมูลปลอมหรือเป็นเท็จ 5) การเข้าถึงโดยมิชอบซึ่งระบบข้อมูลและข้อมูลทางคอมพิวเตอร์ 6) การรีดเอาทรัพย์โดยขู่ว่าจะล่มระบบคอมพิวเตอร์ 7) การใช้หรือมีไว้ซึ่งบัตรอิเล็กทรอนิกส์ของผู้อื่น

8) การหลอกลวงทางอีเมล 9) การหลอกลวงผู้หญิงในการหาคู่ ซึ่งผู้หญิงอายุ 40 ปีขึ้นไปตกเป็นเหยื่อการหลอกลวงหาคู่เพิ่มขึ้นเรื่อยๆ และ 10) การฉ้อโกงในลักษณะอื่น

แผนประทุษกรรมของคนร้ายในคดีหลอกลวงผ่านสื่ออินเทอร์เน็ตที่พบมาก ได้แก่ การสร้างสถานการณ์เร่งด่วนหรือเอาผลประโยชน์มาล่อเพื่อให้เหยื่อโอนเงินหรือบอกข้อมูลส่วนบุคคล ยกตัวอย่าง เช่น อีเมลแจ้งว่าเหยื่อถูกล็อตเตอรี่ออนไลน์ได้รางวัลหลายสิบล้าน แต่ต้องโอนเงินบางส่วนไปเป็นค่าดำเนินการ หรืออาจจะแนบเนียนยิ่งขึ้น เช่น แอบอ้างว่ามาจากธนาคารโดยตั้งชื่ออีเมลคล้ายกับอีเมลของธนาคารจริง จากนั้นก็ขอให้ส่งรหัสผ่านกลับไป หรือในบางกรณีที่คนรู้จักถูกเจาะระบบข้อมูลบัญชีอีเมลเหยื่ออาจได้รับอีเมลแจ้งว่าตอนนี้เขาอยู่ต่างประเทศ และทำกระเป๋าหายขอให้ช่วยโอนเงินไปด่วน การสร้างเว็บไซต์ที่ล่อลวงให้เข้าใจผิดว่าเป็นเว็บไซต์จริง และหลอกให้กรอกข้อมูลส่วนบุคคล เช่น รหัสผ่านหรือเลขบัตรเครดิต การสร้างหน้าจอแจ้งว่าเครื่องคอมพิวเตอร์เหยื่อติดไวรัสคอมพิวเตอร์และให้ดาวน์โหลดและติดตั้งซอฟต์แวร์ต้านไวรัสคอมพิวเตอร์ซึ่งอันจริงแล้วเป็นมัลแวร์(โปรแกรมที่ไม่พึงประสงค์) เพื่อขโมยข้อมูลส่วนบุคคล

จากการสัมภาษณ์เจ้าหน้าที่ตำรวจ พนักงานสอบสวน เจ้าหน้าที่กรมสอบสวนคดี และผู้เชี่ยวชาญคดีอาชญากรรมคอมพิวเตอร์ สามารถนำวิเคราะห์แผนประทุษกรรมอาชญากรรมคอมพิวเตอร์ ที่เกิดขึ้นในสังคมไทยโดยสังเขปที่น่าสนใจมีดังนี้

1. อาชญากรรมที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการหลอกลวง

- แผนประทุษกรรมของคนร้ายคดีแก๊งคอลเซ็นเตอร์

ปัจจุบันแก๊งคอลเซ็นเตอร์ในรูปแบบอาชญากรข้ามชาติ ใช้เป็นช่องทางแอบอ้างและหลอกเหยื่อให้โอนเงินในรูปแบบต่างๆ พฤติการณ์ของ

แก๊งคนร้ายเกือบทั้งหมดเป็นชาวจีน และไต้หวัน ส่วนคนไทยหรือคนชาติอื่นที่เข้าร่วมขบวนการเป็นเพียงพนักงานรับโทรศัพท์กับผู้เปิดบัญชีรับเงินที่ได้จากการล่อลวง การตั้งแก๊งคอลเซ็นเตอร์ มี 2 รูปแบบ คือ 1) ตั้งศูนย์ในประเทศไทยเพื่อโทรกลับไปล่อลวงชาวจีนหรือไต้หวัน โดยเช่าบ้านหรูตามหมู่บ้านในกรุงเทพฯหรือเมืองท่องเที่ยวสำคัญๆ เช่น เชียงใหม่ ภูเก็ต จากนั้นว่าจ้างชาวจีนหรือไต้หวันเข้ามาพักที่บ้าน โดยจะมีอุปกรณ์ต่างๆ ให้พร้อม และติดตั้งระบบโทรศัพท์ข้ามประเทศผ่านอินเทอร์เน็ต หรือ VOIP (Voice over Internet Protocol) โทรกลับไปหลอกเหยื่อชาวจีนหรือไต้หวัน 2) ตั้งศูนย์นอกประเทศไทย ที่ตำรวจเคยจับกุมได้เกือบทั้งหมดอยู่ที่ประเทศจีน โดยศูนย์จะอยู่ตามห้องพักหรือแฟลต มีนายทุนจ้างคนไทยเพื่อทำหน้าที่เป็นคอลเซ็นเตอร์โทรกลับมาหลอกเหยื่อชาวไทย แก๊งคอลเซ็นเตอร์ทั้ง 2 แบบ จะมีการว่าจ้างคนในประเทศนั้นๆ (ประเทศที่โทรไปล่อลวง) ไปเปิดบัญชีธนาคารรอเอาไว้ เช่น หลอกเหยื่อคนไทยก็จะจ้างคนไทยไปเปิดบัญชีธนาคารเอาไว้ จากนั้นจะมี "ม้าวิ่ง" คือชาวจีนหรือไต้หวัน ทำหน้าที่ตระเวนกดเงินตามตู้เอทีเอ็ม เพื่อกดเงินออกจากบัญชีที่เปิดรอไว้ดังกล่าว เมื่อได้เงินมาก็จะส่งเงินต่อไปยังกลุ่มขบวนการด้วยวิธีการต่าง ๆ เช่น รวบรวมเป็นเงินสดนำออกนอกประเทศ หรือนำไปโอนผ่านบัญชีธนาคาร "ม้าวิ่ง" จะเดินทางเข้าออกประเทศมาแล้วหลายครั้ง หลังทำงานเสร็จก็เดินทางกลับ ผู้ต้องหาส่วนใหญ่ที่จับกุมได้ จะเป็นคนที่ทำหน้าที่คอลเซ็นเตอร์, คนไทยที่ถูกจ้างให้เปิดบัญชี และ "ม้าวิ่ง" ที่กดเงินตามตู้เอทีเอ็ม

วิธีการหลอกเหยื่อ จะมีการเขียนสคริปต์ให้คนที่ถูกจ้างมาเป็นคอลเซ็นเตอร์ใช้พูดตามบทที่เขียนขึ้น ซึ่งที่พบมีทั้งภาษาไทยและภาษาจีน ส่วนเนื้อหาในสคริปต์จะมีใจความที่ทำให้เหยื่อเกิดความโลภหรือความหวาดกลัว เช่น ในช่วงที่ประชาชนต้องทำเรื่องเสียภาษี แก๊งคนร้ายก็จะฉวยโอกาสสมอ้างเป็นเจ้าหน้าที่สรรพากรหลอกว่ามีเงินภาษีคืน ให้ไปทำ

ธุรกรรมทางตู้เอทีเอ็ม จะได้สะดวก ได้เงินคืนทันที ไม่ต้องเสียเวลามาทำเรื่องหรืออ้างว่าถูกรางวัลจากการสุ่มเบอร์ ส่วนการหลอกด้วยความหวาดกลัวนั้นมักจะอ้างเป็นเจ้าหน้าที่ธนาคาร เจ้าหน้าที่รัฐ เช่น สำนักงานป้องกันและปราบปรามการฟอกเงิน กรมสอบสวนคดีพิเศษ กรมสรรพากร เจ้าหน้าที่ศาล เนื้อหาหลักๆ จะพุ่งเป้าไปที่บัญชีธนาคารของเหยื่อมีปัญหาต่าง ๆ นานา หลังทำให้เหยื่อเกิดความโลภหรือหวาดกลัวแล้ว ผู้ที่ทำหน้าที่คอลเซ็นเตอร์ก็จะหว่านล้อมด้วยคำพูดแบบหวังดีต้องการช่วยเหลือแต่แท้ที่จริงแล้วประสงค์ร้าย โดยพูดอย่างไรก็ได้ให้เหยื่อไปที่ตู้เอทีเอ็มเพื่อกดโอนเงินไปเข้าบัญชีที่แก๊งคนร้ายเปิดรอไว้แล้ว

กลุ่มแก๊งคอลเซ็นเตอร์ที่ปฏิบัติการหลอกลวงเหยื่อ โดยแบ่งออกเป็น 2 กลุ่ม คือ 1) แก๊งคืนเงินภาษี คนร้ายจะหลอกเหยื่อว่าได้รับภาษีตกค้างคืน เนื่องจากมีการปรับลดหรือเหตุผลอื่นๆ หากต้องการเงินภาษีดังกล่าวต้องรีบดำเนินการภายในวันนี้เท่านั้น แน่นอนว่าเหยื่ออยากได้เงินแต่ไม่มีเวลา คนร้ายจะดำเนินการต่อไปดังนี้ แนะนำให้ไปที่ตู้เอทีเอ็มที่คนร้ายถนัด ทำอย่างไรก็ได้ให้ผู้เสียหายเลือกเมนูภาษาอังกฤษ และพูดโต้ตอบอย่างรวดเร็วให้ผู้เสียหายสับสนจนต้องรีบทำการที่คนร้ายบอก หลอกให้อ่านตัวเลขและโอนเงินของเหยื่อ กว่าเหยื่อจะรู้ตัวว่าถูกหลอกก็ต่อเมื่อโอนเงินไปแล้ว คนร้ายวางหู ในช่วงนี้กว่าเหยื่อจะมีเวลาคิดและรู้ว่าถูกหลอกแต่สายเสียแล้ว 2) แก๊งหนี้บัตรเครดิต คนร้ายจะหลอกเหยื่อว่ามีหนี้บัตรเครดิตจากธนาคารต่างๆ ไม่ว่าเหยื่อจะมีบัตรเครดิตหรือบัญชีของธนาคารนั้นๆ หรือไม่ แน่นอนว่าเหยื่อจะต้องตกใจ จากนั้นคนร้ายจะดำเนินการต่อไปดังนี้ เริ่มหลอกเหยื่อโดยใช้หมายเลขที่ไม่มีในสาระบบ เช่น มีเครื่องหมายบวกอยู่ด้านหน้า หรือเป็นหมายเลขที่ไม่โชว์เบอร์ คนร้ายจะใช้เสียงพูดที่บันทึกเสียงสุภาพสตรีหรือสุภาพบุรุษเลียนแบบทางธนาคาร คนร้ายจะพูดหลอกลวงเหยื่อ เช่น ท่านมีหนี้ค้างบัตรเครดิตของธนาคาร 100,000 บาท ฟังซ้ำกด 1 ภาษา

อังกฤษกด 2 ติดต่อเจ้าหน้าที่กด 9 เมื่อเหยื่อกด 9 จะมีคนร้ายอีกหนึ่งคนพูดจาไพเราะว่าเขาเป็นเจ้าหน้าที่ เพิ่งได้รับโอนสายจากคอลเซ็นเตอร์ไม่ทราบรายละเอียด กรุณาแจ้งชื่อ สกุล เลขบัตรประชาชน อายุ ที่อยู่ เบอร์ที่ทำงาน เลขบัญชีและเลขบัตรเครดิต จากนั้นจะหว่านล้อมอย่างรวดเร็วถึงวิธีการระงับหนี้แบบเร่งด่วนโดยโอนสายไปยังคนร้ายอีกคน คนร้ายคนที่สามจะดำเนินการหลอกเหยื่อโดยแนะนำตนเองว่าเป็นเจ้าหน้าที่ฝ่ายกฎหมายและเร่งรัดหรือประนอมหนี้ธนาคาร ซึ่งพูดจารวดเร็วหว่านล้อมให้รีบระงับหนี้โดยทำธุรกรรมทางโทรศัพท์ หากต้องการให้กดตามที่คนร้ายบอก หรือรีบไปที่ตู้เอทีเอ็ม จากนั้นคนร้ายจะให้เลือกเมนูภาษาอังกฤษ และหลอกให้ผู้เสียหายปฏิบัติตามจนเสร็จสิ้น

- แผนประทุษกรรมของคนร้ายคดีฟิชชิ่ง (Phishing)

ฟิชชิ่ง (Phishing) เป็นการหลอกลวงทางอินเทอร์เน็ตเพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิ่ง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้ผู้เสียหายต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้นมักจะมีหน้าตาคล้ายคลึงกับเว็บไซต์ที่กล่าวถึง โดยการส่งอีเมล หรือปลอมเว็บไซต์เพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคล เช่น รหัสผู้ใช้งาน รหัสผ่าน หรือข้อมูลส่วนบุคคล ที่หลอกลวงมาไปแสวงหาผลประโยชน์

คำว่า Phishing เป็นคำพ้องเสียงจากคำว่า Fishing ซึ่งหมายถึงการตกปลา หากจะเปรียบเทียบเหยื่อล่อที่ใช้ในการตกปลา ก็คือกลวิธีที่ผู้โจมตีใช้ในการหลอกลวงผู้เสียหาย ซึ่งเหยื่อล่อที่เด่นๆ ในการหลอกลวงแบบ Phishing มักจะเป็นการปลอมอีเมล หรือปลอมหน้าเว็บไซต์ที่มีข้อความซึ่งทำให้ผู้เสียหายอ่านแล้วหลงเชื่อ เช่น ปลอมอีเมลว่าอีเมลฉบับนั้นถูกส่งออกมาจากธนาคารที่ผู้เสียหายใช้บริการอยู่ โดยเนื้อความในอีเมล

แจ้งว่าขณะนี้ธนาคารมีการปรับเปลี่ยนระบบรักษาความมั่นคงปลอดภัยของข้อมูลลูกค้า และธนาคารต้องการให้ลูกค้าเข้าไปยืนยันความถูกต้องของข้อมูลส่วนบุคคลผ่านทางลิงก์ที่แนบมาในอีเมล เป็นต้น เมื่อผู้เสียหายคลิกที่ลิงก์ดังกล่าว ก็จะพบกับหน้าเว็บไซต์ปลอมของธนาคารซึ่งผู้โจมตีได้เตรียมไว้ เมื่อผู้เสียหายเข้าไปล็อกอิน ผู้โจมตีก็จะได้ชื่อผู้ใช้และรหัสผ่านของผู้เสียหายไปในทันที การหลอกลวงแบบ Phishing จะอาศัยเหตุการณ์สำคัญที่เกิดในช่วงเวลานั้น ๆ เพื่อเพิ่มโอกาสของการหลอกลวงสำเร็จ เช่น อาศัยช่วงเวลาที่มีภัยธรรมชาติหรือโรคระบาด โดยปลอมเป็นอีเมลจากธนาคารเพื่อขอรับบริจาค เป็นต้น หน้าเว็บไซต์ปลอมบางหน้าจะใช้วิธีการฝังโทรจันที่สามารถขโมยข้อมูลที่ต้องการมากับหน้าเว็บไซต์ปลอมนั้นด้วย เช่น โทรจัน(ไวรัสคอมพิวเตอร์)ทำหน้าที่เป็น Key-logger ซึ่งจะคอยติดตามว่าผู้เสียหายพิมพ์อะไรที่แป้นพิมพ์คอมพิวเตอร์บ้าง เป็นต้น เมื่อผู้เสียหายกดลิงก์ตามเข้ามาที่หน้าเว็บไซต์ปลอมก็จะติดโทรจันโดยอัตโนมัติ และหากผู้เสียหายทำการล็อกอินเข้าใช้งานระบบใด ข้อมูลชื่อผู้ใช้ และรหัสผ่าน ของระบบนั้นก็จะถูกส่งไปยังคนร้าย

- แผนประทุษกรรมของคนร้ายในคดีไนจีเรียนสแกม

ไนจีเรียนสแกม (Nigerian scams) คือ การหลอกลวงจากกลุ่มอาชญากรชาวไนจีเรีย เสนอเงินจำนวนมากให้กับผู้เสียหายผ่านทางอีเมลหรือโซเชียลมีเดีย(Social media) โดยมีเงื่อนไขให้ผู้เสียหายโอนเงินออกนอกประเทศ คนร้ายจะสร้างเรื่องราวหลากหลายรูปแบบ เช่น อ้างว่าตนมีเงินจำนวนมากในธนาคารแต่ไม่สามารถนำออกมาได้เพราะประเทศกำลังเผชิญกับสงครามกลางเมืองหรือรัฐประหาร(มักเป็นประเทศที่กำลังเป็นข่าวอยู่) ขอให้ช่วยโอนเงินมาเพื่อใช้ปลดล็อกบัญชีแล้วจะให้รางวัลจำนวนมากในภายหลัง

เทคนิคของคนร้ายใช้หลอกล่อเหยื่อ คนร้ายมักจะแอบอ้างเป็นนักกฎหมาย นายธนาคาร หรือ ข้าราชการ เพื่อสร้างความน่าเชื่อถือมากยิ่งขึ้น เพื่อสร้างความแนบเนียนให้เหยื่อผู้เคราะห์ร้ายตายใจ คนร้ายมักจะใช้ประโยควิธีการโน้มน้าวต่อเหยื่อ เพื่อให้เหยื่อหลงผิด ถึงการหลอกลวงจนนำไปสู่ขั้นตอนการทำธุรกรรมการเงิน คนร้ายมักจะวางกับดักวิธีการเพื่อให้ได้มาซึ่งเงินของเหยื่อด้วยเทคนิคการแอบอ้างข้างต้น โดยใช้จุดอ่อนของเหยื่อที่เป็นคนหลงเชื่อคนง่าย หรือ การสุ่มผู้คนเป็นปริมาณมากซึ่งต้องมีบางส่วนที่หลงเชื่อแม้เพียงเล็กน้อยก็ตาม การหลอกลวงอาจมาในรูปแบบที่ไม่คาดคิด เช่น การได้รับรางวัลใหญ่ไม่ว่าจะเป็นการถูกลอตเตอรี่ การได้รับรางวัลการท่องเที่ยวไปต่างประเทศ หรือการได้รับของรางวัลที่มีมูลค่าดึงดูดใจ

- แผนประทุษกรรมคดีแชร์ลูกโซ่ ลักษณะคล้ายกับรูปแบบของแชร์ลูกโซ่ในอดีตที่ผ่านมาเพียงแต่นำสื่ออินเทอร์เน็ตมาเป็นเครื่องมือในการหลอกลวงให้ผู้เสียหายตกเป็นเหยื่อ แยกเป็น 2 ระดับ คือ

1) ระดับล่าง คือ การชักชวนให้เล่นแชร์ลูกโซ่ผ่านสื่ออินเทอร์เน็ต เช่น เฟซบุ๊ค ไลน์ แชร์ทองคำ แชร์เงินสด ที่จะเน้นการชักชวนโดยไม่เคยเห็นหน้าตาของสมาชิกมาก่อนแต่เน้นเรื่องให้ผลตอบแทนมาก โดยผู้กระทำผิดใช้สื่ออินเทอร์เน็ตเป็นเครื่องมือในการหลอกลวงให้เล่นแชร์ มีผู้ที่ตกเป็นเหยื่อจำนวนหลายร้อยคน โดยที่ไม่สามารถตามจับได้และได้ทำการเปลี่ยนชื่อเปลี่ยนกลุ่มไลน์ไปหลอกลวงเหยื่อคนอื่นต่อไป

2) ระดับบน คือ การจัดอบรมสัมมนาให้ความรู้เรื่องการซื้อขายหุ้น การซื้อขายทองคำ การลงทุนในเงินดิจิตอล หรือการลงทุนทำธุรกิจต่างๆ ในต่างประเทศมักจะเป็นองค์กรอาชญากรรมข้ามชาติมีเครือข่ายหลายประเทศ มีมูลค่าความเสียหายมากกว่าและผู้ที่ตกเป็นเหยื่อมักจะเป็นคนรวย หรือนักธุรกิจ หรือกลุ่มข้าราชการที่เกษียณอายุที่ได้รับเงินบำนาญมาแล้วอยากจะให้เงินงอกเงย ซึ่งในปัจจุบันการเล่นแชร์ลูกโซ่ในระดับสูง

ได้รับความนิยมเป็นอย่างมาก ดังจะเห็นได้จากตัวอย่าง คดีแชร์ลูกโซ่ยูฟัน ที่มีผู้ตกเป็นเหยื่อหลายหมื่นคน ลักษณะหรือกระบวนการทำให้ตกเป็นเหยื่อ คือ จัดอบรมสัมมนาในโรงแรมใหญ่ สร้างความน่าเชื่อถือ แสดงให้สมาชิกหรือคนที่มาเข้าฟังเห็นว่าผลตอบแทนที่จะได้รับมีอะไรบ้างจากการลงทุน จนประชาชนหลงเชื่อร่วมลงทุนและตกเป็นเหยื่อแชร์ลูกโซ่ มูลค่าความเสียหายเป็นหมื่นล้านบาท

2. **อาชญากรรมที่โจมตีต่อระบบและข้อมูลคอมพิวเตอร์**

- แผนประทุษกรรมของการโจมตีของมัลแวร์เรียกค่าไถ่ (Ransomware)

การโจมตีของมัลแวร์เรียกค่าไถ่ (Ransomware) มีการเพิ่มจำนวนอย่างต่อเนื่องจนกลายเป็นปัญหาระดับโลก และเป็นช่องทางทำเงินให้กับอาชญากร ปี 2560 มีมัลแวร์เรียกค่าไถ่รุ่นใหม่ กว่า 101 ชนิด ถูกปล่อยออกมา ซึ่งเพิ่มขึ้นกว่า 3 เท่าเมื่อเทียบกับปี 2559 ที่มีมัลแวร์เรียกค่าไถ่รุ่นใหม่ถูกปล่อยออกมาประมาณ 30 ชนิด ซึ่งประเทศอเมริกาเป็นเป้าหมายหลักที่ถูกโจมตีจากมัลแวร์เรียกค่าไถ่ พบว่า 64 % ของคนอเมริกัน ที่ตกเป็นเหยื่อของมัลแวร์เรียกค่าไถ่ ยอมที่จะจ่ายเงินให้คนร้ายเพื่อแลกกับการได้ข้อมูลคืน ซึ่งค่าไถ่ที่อาชญากรเรียก ประมาณ 1,077 ดอลลาร์จากเหยื่อแต่ละราย ขณะที่มูลค่าการเรียกค่าไถ่ข้อมูลสูงสุดอยู่ที่ 28,730 ดอลลาร์ สำหรับประเทศไทยมีผู้ที่ถูกโจมตีแล้ว แต่ยังไม่มีการเก็บข้อมูลที่แน่ชัด โดยประเทศไทยถูกจัดให้อยู่ในอันดับที่ 12 ของเป้าหมายในการถูกโจมตีในระดับภูมิภาค และอยู่ในอันดับที่ 34 ในระดับโลก ซึ่งในระดับโลกไทยถูกจัดอันดับความเสี่ยงเพิ่มขึ้น เนื่องจากปี 2558 ไทยอยู่ในอันดับที่ 46 ของการตกเป็นเป้าถูกโจมตี (MGROnline, 2560)

มัลแวร์เรียกค่าไถ่ชื่อ WannaCry มีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลในคอมพิวเตอร์เพื่อเรียกค่าไถ่ หากไม่จ่ายเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้ สิ่งที่น่ากังวลสำหรับมัลแวร์ชนิดนี้ คือความสามารถในการกระจายตัวเองจากเครื่องคอมพิวเตอร์หนึ่งไปยังเครื่องคอมพิวเตอร์อื่นๆ ในเครือข่ายได้โดยอัตโนมัติ ผ่านช่องโหว่ระบบ SMB (Server Message Block) ของระบบปฏิบัติวินโดวส์ ผู้ใช้งานที่ไม่อัปเดตระบบปฏิบัติการวินโดวส์มีความเสี่ยงที่จะติดมัลแวร์ชนิดนี้ ช่องโหว่ที่ถูกใช้ในการแพร่กระจายมัลแวร์เป็นช่องโหว่ที่ถูกเปิดเผยสู่สาธารณะตั้งแต่ช่วงเดือนเมษายน 2560 และถึงแม้ทางบริษัท Microsoft จะเผยแพร่โปรแกรมอัปเดตแก้ไขช่องโหว่ดังกล่าวไปตั้งแต่วันที่ 14 มีนาคม 2560 แต่ก็ยังพบว่าปัจจุบันมีเครื่องคอมพิวเตอร์ที่ยังไม่ได้อัปเดตโปรแกรมแพตช์ดังกล่าวและถูกโจมตีจากมัลแวร์ชนิดนี้มากกว่า 200,000 เครื่อง จาก 112 ประเทศ โดยเกิดผลกระทบสูงต่อหน่วยงานสาธารณสุขของประเทศอังกฤษ ในประเทศไทยพบเครื่องคอมพิวเตอร์มัลแวร์ชนิดนี้ในจำนวนน้อย (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย ,2560)

- แผนประทุษกรรมคดีปล่อยมัลแวร์ฝังในระบบเอทีเอ็มของธนาคาร

การโจรกรรมเงินจากตู้เอทีเอ็มโดยใช้มัลแวร์ (โปรแกรมที่ไม่พึงประสงค์) เจาะระบบเป็นครั้งแรกของประเทศไทย ข้อมูลจากการสืบสวนคาดว่ากลุ่มคนร้ายเป็นชาวยุโรปตะวันออก เช่น รัสเซีย โรมาเนีย เข้ามาปฏิบัติการในประเทศไทย โดยเลือกเจาะระบบที่ตู้เอทีเอ็มด้วยการฝังมัลแวร์เข้าไปในระบบของธนาคาร จากนั้นคนร้ายจะนำบัตรแถบแม่เหล็กที่ทำขึ้นเฉพาะไปตระเวนกดเงินสดจากตู้เอทีเอ็มของธนาคารดังกล่าวในพื้นที่

6 จังหวัด ได้แก่ กรุงเทพฯ เพชรบุรี ชุมพร ประจวบคีรีขันธ์ ภูเก็ต และสุราษฎร์ธานี จำนวนเงินกว่า 12.2 ล้าน จากการสืบสวนพบว่าพฤติกรรมของคนร้ายกลุ่มนี้เชื่อมโยงกับคดีที่เกิดขึ้นในประเทศไต้หวัน โดยอาชญากรจากยุโรปและรัสเซีย โดยใช้มัลแวร์เจาะระบบข้อมูลขโมยเงินธนาคารจากตู้เอทีเอ็มหลายแห่ง รวมมูลค่า 2.5 ล้านดอลลาร์สหรัฐ หรือประมาณ 86 ล้านบาท ซึ่งเจ้าหน้าที่สันนิษฐานว่าคนร้ายใช้โทรศัพท์มือถือเป็นอุปกรณ์ในการเจาะระบบด้วยวิธีการต่อสาย USB เพื่อปล่อยมัลแวร์โดยตรงกับตู้เอทีเอ็ม เหมือนที่เกิดขึ้นในประเทศไต้หวัน

- แผนประทุษกรรมคดีโจมตีเพื่อเปลี่ยนแปลงข้อมูลหน้าเว็บไซต์

ภัยคุกคามรูปแบบหนึ่งที่มักจะเกิดขึ้นกับบริการเว็บไซต์ คือ การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลเผยแพร่หน้าเว็บไซต์ (Website Defacement) ซึ่งผู้โจมตีมีวัตถุประสงค์เพื่อปรับเปลี่ยนหน้าเว็บไซต์แรกของเว็บไซต์เป้าหมาย หรือทั้งเว็บไซต์ จากเดิมไปเป็นหน้าเว็บไซต์ใหม่ การกระทำเช่นนี้อาจไม่ได้ก่อความเสียหายที่รุนแรงอะไรมากนัก เพียงแต่มีความต้องการเพื่อทำลายความน่าเชื่อถือของหน่วยงานเจ้าของเว็บไซต์ ซึ่งในเว็บไซต์ที่ถูกโจมตีส่วนใหญ่จะปรากฏรูปภาพหรือข้อความที่บ่งบอกถึงว่าเว็บไซต์ได้ถูกโจมตีได้สำเร็จ

วิธีการหรือเทคนิคที่ผู้โจมตี โดยการเข้าปรับเปลี่ยนข้อมูลบนหน้าเว็บไซต์ได้ มีอยู่หลายวิธี เช่น การโจมตีต่อเว็บไซต์โดยตรง การโจมตีต่อระบบปฏิบัติการของเครื่องแม่ข่าย(Web Server) ที่ให้บริการเว็บไซต์จนสามารถเข้าควบคุมการทำงานของเครื่องแม่ข่ายบริการเว็บไซต์ได้ ส่งผลให้ผู้โจมตีสามารถเข้าปรับเปลี่ยนข้อมูลในเว็บไซต์เป้าหมายได้ตามต้องการ

3. อาชญากรรมที่ใช้คอมพิวเตอร์และอินเทอร์เน็ตในการล่วงละเมิดทางเพศต่อเด็ก

- แผนประทุษกรรมการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต

ผู้ค้าประเวณีเด็กนิยมใช้เครือข่ายอินเทอร์เน็ต ชักชวนเด็ก รวมถึงการติดต่อเด็กโดยตรง หรือเว็บไซต์ที่เสนอบริการทางเพศของเด็ก ซึ่งผู้กระทำผิดทางเพศต่อเด็กมักบันทึกการกระทำผิดของตนไว้และแบ่งปันสื่อลามกอนาจารเด็กที่ตนทำขึ้นมานั้นกับผู้กระทำผิดคนอื่นผ่านสื่ออินเทอร์เน็ต และโซเชียลมีเดีย ผู้กระทำผิดมีการครอบครองและเผยแพร่สื่อลามกเด็ก เป็นความผิดตามประมวลกฎหมายอาญา มาตรา 287/1 และ 287/2 เพื่อทำให้เด็กเชื่อว่ากิจกรรมทางเพศระหว่างเด็กกับผู้ใหญ่นั้นเป็นเรื่องปกติ ซึ่งรวมไปถึงการเดินทางไปยังประเทศจุดหมายเพื่อร่วมกิจกรรมทางเพศกับเด็ก และยังมีการซื้อบริการล่วงละเมิดทางเพศเด็กออนไลน์ด้วย กรณีนี้ผู้กระทำความผิดจะซื้อบริการทางเพศเด็กผ่านเว็บแคมแบบเรียลไทม์

การปราบปรามการล่วงละเมิดทางเพศเด็กผ่านสื่ออินเทอร์เน็ตในประเทศไทย เน้นการสืบสวนแฝงตัวเข้าไปในกลุ่มสื่อออนไลน์ต่างๆ เพื่อหาข้อมูลสำหรับป้องกันและปราบปรามคดีล่วงละเมิดทางเพศ โดยเฉพาะกลุ่มเด็กและเยาวชน ที่มักตกเป็นเหยื่อคดีทางเพศ และปัจจุบันสื่ออินเทอร์เน็ตเข้าถึงได้ง่าย กลุ่มผู้กระทำผิดเปลี่ยนพฤติกรรมใช้สื่ออินเทอร์เน็ตเป็นช่องทางในการล่อลวงผู้เสียหายมากขึ้น การล่อลวงเด็กและเยาวชนถ่ายคลิปทางเพศเผยแพร่ในสื่ออินเทอร์เน็ตยังต้องสืบสวนหาตัวผู้กระทำผิด ส่วนแนวโน้มเชื่อว่ายังมีการลักลอบกระทำผิดอีกจำนวนมาก

สำหรับสถิติการจับกุมแบ่งตามฐานความผิด ของคณะทำงานปราบปรามการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต หรือ ไทแคค (TICAC) ระหว่างปี 2558 - 2561 จับผู้กระทำผิดคดีค้ามนุษย์ จำนวน 21 คดี, คดีล่วงละเมิดทางเพศเด็ก จำนวน 13 คดี, คดีครอบครองสื่อลามกอนาจารเด็ก

จำนวน 31 คดี และส่งกลับออกนอกราชอาณาจักร จำนวน 6 คดี พบว่า ผู้กระทำความผิดเป็นผู้ต้องหาชาวไทย จำนวน 38 คน และผู้ต้องหาต่างชาติ จำนวน 35 คน จากทั้งหมด 71 คดี ของกลางที่ตรวจยึดได้ที่เป็นไฟล์รูปภาพหรือวีดีโอของผู้เสียหาย เป็นจำนวนมากกว่า 100 GB ซึ่งต้องอาศัยความชำนาญในการคัดแยกเหยื่อและติดตามผู้เสียหายของผู้ที่มีความเชี่ยวชาญ

แนวทางการสืบสวนคดีอาชญากรรมคอมพิวเตอร์

ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 2(10) ได้ให้คำนิยามไว้ว่า "การสืบสวน" หมายความถึงการแสวงหาข้อเท็จจริงและหลักฐาน ซึ่งพนักงานฝ่ายปกครองหรือตำรวจได้ปฏิบัติไปตามอำนาจและหน้าที่เพื่อรักษาความสงบเรียบร้อยของประชาชน และเพื่อที่จะทราบรายละเอียดแห่งความผิด

จะเห็นได้ว่า การสืบสวน สามารถดำเนินการได้ทั้งก่อนการกระทำผิดและหลังกระทำผิด โดยที่กรณีก่อนการกระทำผิดเป็นการทำไปเพื่อรักษาความสงบเรียบร้อย เช่น การส่งตำรวจสายตรวจออกพื้นที่เพื่อหาข่าวและป้องกันปราบปรามจับกุมผู้กระทำความผิด เป็นต้น ส่วนการสืบสวนหลังกระทำผิดเป็นการแสวงหาข้อเท็จจริงและหลักฐานเพื่อทราบรายละเอียดแห่งความผิด

จากสัมภาษณ์กลุ่มตัวอย่าง พบว่า การสืบสวนคดีอาชญากรรมคอมพิวเตอร์โดยส่วนใหญ่ สืบสวนจากข้อมูลการเชื่อมต่ออินเทอร์เน็ต ข้อมูลการเชื่อมต่อโทรศัพท์มือถือ ข้อมูลการใช้งานอีเมล ข้อมูลการใช้งานโซเชียลมีเดีย ข้อมูลการใช้งานบัตรเครดิต ข้อมูลการโอนเงินจากทางธนาคาร ข้อมูลจากกล้องวงจรปิด แผนประทุษของคนร้าย ระบบภูมิศาสตร์สารสนเทศ ความร่วมมือการประสานทั้งระหว่างหน่วยงานในประเทศและระหว่างประเทศ การวางแผนการสืบสวน การวางแผนการจับกุม การตรวจค้นผู้ต้องหา

การรวบรวมพยานหลักฐาน การตรวจพิสูจน์วัตถุพยานทางดิจิทัล ได้แก่ การตรวจพิสูจน์เครื่องคอมพิวเตอร์ การตรวจพิสูจน์เครื่องโทรศัพท์มือถือ ตามหลักการห่วงโซ่การคุ้มครองพยานหลักฐาน (Chain of custody)

แนวทางการเพิ่มประสิทธิภาพการสืบสวนคดีอาชญากรรมคอมพิวเตอร์

1) ด้านการกำหนดภาระความรับผิดชอบ ได้แก่ การกำหนดประเภทของคดีตามลำดับความสำคัญ เช่น จำนวนผู้เสียหาย จำนวนมูลค่าความเสียหาย หรือความซับซ้อนของคดีให้มีความชัดเจนว่าให้หน่วยงานใดเป็นผู้ดำเนินการสืบสวนสอบสวน พร้อมทั้งกำหนดให้แต่ละหน่วยรวบรวมฐานข้อมูลผู้เชี่ยวชาญ ด้านต่างๆ ของอาชญากรรมคอมพิวเตอร์ขึ้นทะเบียนเพื่อสร้างฐานข้อมูล ให้คำปรึกษากับเจ้าหน้าที่สืบสวนสอบสวนในด้านการพิสูจน์หลักฐาน

2) ด้านการสร้างความตระหนักรู้ ในระดับของเจ้าหน้าที่สืบสวนรายบุคคลว่าการสืบสวนสอบสวนในสภาวะแวดล้อมใหม่ที่มีการเปลี่ยนแปลงในส่วนของบริบททางด้านสังคมเศรษฐกิจ อย่างรวดเร็ว อาชญากรรมคอมพิวเตอร์เป็นเรื่องที่เกิดขึ้นได้เป็นการทั่วไป มีการพัฒนาการอย่างรวดเร็วตามการเปลี่ยนแปลงของโลกดังกล่าว ดังนั้น เจ้าหน้าที่สืบสวนมีความจำเป็นต้องมีความรู้ความเข้าใจในเรื่องดังกล่าว ไม่ว่าจะเป็นเรื่องผู้ให้บริการการเก็บเนื้อหาบนอินเทอร์เน็ต หรือหลักฐานทางอิเล็คทรอนิคส์ เช่น ข้อมูลจราจรทางคอมพิวเตอร์ (log file)

3) ด้านการคัดสรรบุคลากร ได้แก่ การคัดสรรบุคลากรเข้าสู่ระบบและการพัฒนาอย่างต่อเนื่อง เจ้าหน้าที่สืบสวนควรมีการทดสอบความรู้ด้านคอมพิวเตอร์พื้นฐาน เช่น ความรู้เรื่องข้อเท็จจริงทางดิจิทัล(Digital Fact) การแยกและการสร้างความเข้าใจในองค์ประกอบของการกระทำ

ความผิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์เช่น การเข้าถึง การทำให้เปลี่ยนแปลง การทำให้เสียหาย ด้วยวิธีการทางดิจิทัล(Digital Way) รวมทั้ง การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ

4) ด้านการเสริมสร้างความรู้ ได้แก่ การสร้างเสริมความรู้ด้านอาชญากรรมคอมพิวเตอร์อย่างต่อเนื่อง โดยหน่วยงาน ทั้งในส่วนของการศึกษาอบรมก่อนการปฏิบัติงาน หรือ การอบรมระหว่างการปฏิบัติงาน (On the Job Training) ควรกำหนดไว้ในหลักสูตรแกนกลาง ในส่วนการพิสูจน์หลักฐานทางคอมพิวเตอร์ที่เป็นหัวใจสำคัญในการสืบสวนสอบสวน

5) ด้านการพัฒนาเครื่องมือวัสดุครุภัณฑ์ ได้แก่ การจัดหาวัสดุอุปกรณ์เพื่อช่วยในการสืบสวนสอบสวนอาชญากรรมคอมพิวเตอร์ในระดับผู้เชี่ยวชาญ เช่น อุปกรณ์การจัดเก็บสำเนาข้อมูลอิเล็กทรอนิกส์

แนวทางการระวังป้องกันภัยอาชญากรรมคอมพิวเตอร์

การป้องกันอาชญากรรมที่ใช้คอมพิวเตอร์ในการหลอกลวง

1) จากการสัมภาษณ์ผู้เชี่ยวชาญ พบว่า การป้องกันอาชญากรรมคอมพิวเตอร์โดยการลดโอกาสการตกเป็นเหยื่อ การสร้างภูมิคุ้มกันให้กับประชาชนได้รู้จักการป้องกันและระวังภัยด้วยตนเอง รวมทั้งกระตุ้นให้เกิดการเรียนรู้ถึง รูปแบบ วิธีการของภัยอาชญากรรม โดยเน้นการประชาสัมพันธ์เพื่อให้ความรู้ ข้อมูลข่าวสาร ที่เป็นประโยชน์ในการไม่ให้ตกเป็นเหยื่ออาชญากรรม ได้แก่ การจัดให้มีระบบเตือนภัยอาชญากรรมสำหรับประชาชนในรูปแบบต่างๆ การพัฒนาระบบศูนย์รับแจ้งเหตุ รวมทั้งมีเจ้าหน้าที่หรือชุดปฏิบัติการที่มีความพร้อมสามารถตอบสนองการรับแจ้งเหตุเข้าไปช่วยเหลือและแก้ปัญหาได้ทันเหตุการณ์ การผลิตสื่อประชาสัมพันธ์เพื่อให้ความรู้กับประชาชน โดยเฉพาะกลุ่มเสี่ยงที่มีโอกาสเป็นเป้าหมายของอาชญากร อาทิ เด็ก สตรี คนชรา ในลักษณะหลากหลายรูปแบบให้มีความเหมาะสม

กับแต่ละกลุ่มเป้าหมาย โดยให้ความรู้ในเรื่องของรูปแบบ ลักษณะวิธีการในการก่ออาชญากรรม เช่น วิธีป้องกันการหลอกลวงผ่านทางอินเทอร์เน็ต ตัวอย่างที่พบบ่อย หลอกว่าเป็นผู้โชคดีเพื่อล้วงข้อมูลส่วนตัว หรือหลอกเป็นชาวต่างชาติเพื่อขอแต่งงาน ส่วนใหญ่จะมาจากการสนทนาทางโปรแกรมแชท ให้ข้อมูลส่วนตัว เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ หรือนัดเจอคนที่รู้จักกันทางอินเทอร์เน็ตอาจตกเป็นเหยื่อของคนเหล่านี้ได้ วิธีการป้องกันคือไม่ส่งหลักฐานส่วนตัวของตนเองและคนในครอบครัวให้ผู้อื่น การไม่ออกไปพบคนที่รู้จักทางอินเทอร์เน็ตเพื่อป้องกันการลักพาตัว โดยระลึกอยู่เสมอว่าบุคคลที่รู้จักทางอินเทอร์เน็ตอาจจะเป็นคนร้าย

2) วิธีป้องกันการหลอกลวง แบบ Phishing ไม่เปิดลิงก์ที่แนบมาในอีเมล์ ระวังอีเมลที่ขอให้กรอกข้อมูลส่วนบุคคล โดยเฉพาะหากเป็นอีเมล์ที่มาจากสถาบันการเงินสังเกตให้แน่ใจว่าเว็บไซต์ที่ใช้งานเป็น HTTPS ก่อนให้ข้อมูลส่วนบุคคลที่สำคัญ

การป้องกันอาชญากรรมที่มุ่งโจมตีระบบและข้อมูลคอมพิวเตอร์

1) วิธีการป้องกันการเจาะระบบคอมพิวเตอร์ระดับหน่วยงาน หรือระดับองค์กร ต้องมีการจัดหาระบบ Firewall เพื่อป้องกันการโจมตีหรือการเจาะระบบ ทำการปรับปรุงระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายและปรับปรุงโปรแกรมป้องกันไวรัสคอมพิวเตอร์ให้เป็นรุ่นปัจจุบัน

2) วิธีการป้องกันมัลแวร์(Malware) อัพเดทระบบปฏิบัติการคอมพิวเตอร์และซอฟแวร์ในเครื่องคอมพิวเตอร์ให้เป็นรุ่นปัจจุบัน ติดตั้งโปรแกรมป้องกันมัลแวร์(Anti-malware) บนเครื่องคอมพิวเตอร์ และระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อ ไม่กดปุ่มข้อความที่แสดงโฆษณาหรือหน้าต่าง ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือที่เสี่ยงต่อ

การมีมัลแวร์แฝงอยู่ หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ส่งมาจากอีเมลที่ไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

3) วิธีการป้องกันเทคนิคการตั้งรหัสผ่าน(Password) ที่มีความปลอดภัย

- รหัสผ่านควรมีความยาวอย่างน้อย 8 อักขระ ขึ้นไป
- สร้างรหัสที่ประกอบด้วยตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์ ผสมกัน
- หลีกเลี่ยงการใช้ข้อมูลส่วนตัวที่คาดเดาได้ง่ายและไม่เป็นความลับ เช่น วันเกิด ทะเบียนรถ หมายเลขโทรศัพท์ ชื่อเล่น ชื่อสัตว์เลี้ยง
- เปิดใช้ระบบการพิสูจน์ตัวตนที่ปลอดภัยมากขึ้น ได้แก่ การพิสูจน์ตัวตนสองระดับ(two-factor authentication) คือ ระบบที่ต้องพิสูจน์ตัวตนสองประเภทก่อนจึงจะล็อกอินเข้าระบบได้ เช่น รหัสผ่านและลายนิ้วมือ นอกจากจะต้องใส่รหัสผ่านแล้วระบบจะส่งรหัสเฉพาะทางโทรศัพท์มือถือ (เรียกว่า OTP) เพื่อใช้ยืนยันตัวตนอีกขั้นหนึ่ง

4) วิธีการป้องกันข้อมูลสำคัญเมื่อจำเป็นต้องใช้อินเทอร์เน็ตสาธารณะ

- การใช้งานเครื่องคอมพิวเตอร์ของห้องสมุด เครื่องคอมพิวเตอร์ของร้านอินเทอร์เน็ตคาเฟ่ หรือโทรศัพท์มือถือของเพื่อน หลีกเลี่ยงการล็อกอินเข้าบริการที่สำคัญ เช่น อีเมล โซเชียลมีเดีย และธนาคารออนไลน์
- ออกจากระบบทุกครั้งหลังใช้งานและไม่ตั้งค่าให้เครื่องจำรหัสผ่านหรือสถานะของผู้ใช้
- พยายามหลีกเลี่ยงการใช้งาน Free wifi ในการใช้งานบริการสำคัญ เช่น การลงชื่อเข้าใช้บัญชีอีเมล การโอนเงินผ่านระบบธนาคารออนไลน์ เนื่องจากอาจมีคนร้ายดักรับข้อมูลรหัสผ่าน

การป้องกันอาชญากรรมที่ใช้คอมพิวเตอร์และอินเทอร์เน็ตในการล่วงละเมิดทางเพศต่อเด็ก

1) ภาครัฐควรทำกิจกรรมส่งเสริมให้ประชาชนตระหนักถึงภัยทางอินเตอร์เน็ตเกี่ยวกับการล่วงละเมิดทางเพศต่อเด็ก การผลิตสื่อประชาสัมพันธ์เพื่อให้ความรู้กับประชาชน โดยเฉพาะกลุ่มเสี่ยงที่มีโอกาสเป็นเป้าหมายของอาชญากร

2) ผู้ปกครองควรให้คำแนะนำการใช้งานบนอินเทอร์เน็ตอย่างถูกวิธีแก่บุตรหลาน เพื่อไม่ให้ตกเป็นเหยื่อของการล่วงละเมิดทางเพศ

3) การจัดทำฐานข้อมูลผู้กระทำผิดทางเพศต่อเด็ก พร้อมประวัติทางอาชญากรรมของผู้ที่ถูกปล่อยตัวเมื่อพ้นโทษในคดีความผิดเกี่ยวกับเพศ ซึ่งรัฐบาลของหลายประเทศเห็นว่า มาตรการนี้จะช่วยให้เจ้าหน้าที่ตำรวจหรือหน่วยงานที่เกี่ยวข้องสามารถติดตามตรวจสอบความเคลื่อนไหวของผู้กระทำผิดทางเพศได้อย่างต่อเนื่องอันเป็นการลดความเสี่ยงการเกิดอาชญากรรม

บทสรุป

อาชญากรรมบนอินเทอร์เน็ตเกิดขึ้นได้ทุกที่ทุกเวลาตามแต่โอกาสของผู้กระทำผิดตัดสินใจลงมือก่ออาชญากรรม อีกทั้งในปัจจุบันการเปลี่ยนแปลงของสังคมทำให้รูปแบบของอาชญากรรมเกิดขึ้นอย่างหลากหลาย มีวิธีการกระทำความผิดที่ซับซ้อน โดยนำเอาลักษณะของการประกอบธุรกิจหรือเทคโนโลยีในรูปแบบต่างๆ มาผสมผสานกับการกระทำความผิดเพิ่มมากขึ้น ทำให้ยากต่อการสืบสวนจับกุมและการบังคับใช้กฎหมาย และในบางครั้งมีการดำเนินงานในลักษณะองค์กรอาชญากรรมนำไปสู่รูปแบบของอาชญากรรมข้ามชาติส่งผลกระทบและสร้างความเสียหายต่อเนื่องหลายประเทศ

ความเสียหายทางทรัพย์สินคดีอาชญากรรมคอมพิวเตอร์ในช่วงปี 2561 ความผิดเกี่ยวกับการฉ้อโกงประชาชนผ่านสื่อสังคมออนไลน์ คิดเป็นมูลค่า 3,000 ล้านบาท คดีโรแมนซ์ สแกม (Romance scam) ความเสียหายคิดเป็นมูลค่า 85,529,454 บาท โดยยึดและอายัดทรัพย์สิน คืนเงินให้แก่ผู้เสียหาย รวมเป็นเงินกว่า 2,085,000 บาท คดีแก๊งคอลเซ็นเตอร์สร้างความเสียหาย คิดเป็นมูลค่า 259,294,632 บาท คดีการพนันออนไลน์ คิดเป็นมูลค่า 20 ล้านบาท ถือเป็นความเสียหายต่อระบบเศรษฐกิจของประเทศอย่างมาก กระทบต่อความปลอดภัยสาธารณะ(Public Safety)

นอกจากมูลค่าความเสียหายที่นับเป็นจำนวนเงิน ยังมีความเสียหายที่ส่งผลกระทบทางจิตใจที่เกี่ยวเนื่องกับคดีอาชญากรรมคอมพิวเตอร์ เช่น คดีเผยแพร่สื่อลามกเด็กและการละเมิดทางเพศเด็ก หากพิจารณาโดยอาศัยหลักทางการจิตวิทยา จะเห็นได้ว่าความเสียหายที่เกิดขึ้นต่อเหยื่ออาชญากรรมก่อให้เกิดความทุกข์ทรมาน เกิดความวิตกกังวล อารมณ์เศร้า อาจส่งผลกระทบต่อเหยื่อเป็นเวลานานกว่าความเสียหายอย่างอื่นที่คำนวณเป็นจำนวนเงิน เด็กที่ตกเป็นเหยื่อเหล่านี้หากไม่ได้รับการดูแลเอาใจใส่ บางส่วนมีแนวโน้มที่จะกลายเป็นผู้ใหญ่ซึ่งก่อปัญหาอาชญากรรมในลักษณะเดียวกัน

แนวทางการป้องกันอาชญากรรมบนอินเทอร์เน็ต ภาครัฐควรประชาสัมพันธ์การสร้างความเข้าใจให้กับประชาชนตระหนักถึงภัยอาชญากรรมที่เกิดขึ้น การผลิตสื่อประชาสัมพันธ์เพื่อให้ความรู้กับประชาชน โดยเฉพาะกลุ่มเสี่ยงที่มีโอกาสเป็นเป้าหมายของอาชญากร การพัฒนาศักยภาพบุคลากรในหน่วยงานบังคับใช้กฎหมายให้มีทักษะและความรู้ความสามารถ การรวบรวมแผนประทุษกรรมของคนร้ายเพื่อพัฒนาความรู้ด้านการสืบสวนสอบสวน การส่งเสริมความร่วมมือเชิงวิชาการโดยเน้นการศึกษาวิจัยแลกเปลี่ยนความรู้และผลการศึกษาวิจัย การสร้างความร่วมมือด้านการสืบสวนอาชญากรรม

คอมพิวเตอร์ระหว่างหน่วยงานทั้งในและต่างประเทศ การเตรียมความพร้อมรับสถานการณ์การเฝ้าระวังการโจมตีระบบคอมพิวเตอร์ การพัฒนางานพิสูจน์พยานหลักฐานทางดิจิทัล

เอกสารอ้างอิง

กองบัญชาการตำรวจท่องเที่ยว. (2561). แถลงผลงานสำนักงานตำรวจแห่งชาติ ประจำปี 2561. สืบค้นเมื่อ 28 กันยายน 2561 , จาก https://touristpolice.go.th/2018/09/28/

กองปราบปราม กองบัญชาการสอบสวนกลาง. (2555). การบริหารงานสืบสวน. สืบค้นเมื่อ 6 มีนาคม 2561 , จาก http://www.csd.go.th/dimensions_csd/4dimensions-2.pdf

สฤษดิ์ สืบพงษ์ศิริ. (2558). การจำลองภาพอาชญากรรมเพื่อเชื่อมโยงเหตุการณ์ในแนวทางด้านนิติวิทยาศาสตร์. วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

สฤษดิ์ สืบพงษ์ศิริ. (2560). แผนประทุษกรรมกับลายเซ็นอาชญากรรมของคนร้าย : ความเหมือนที่แตกต่าง. วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์ โรงเรียนนายร้อยตำรวจ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT). (2560). สถิติภัยคุกคาม.สืบค้นเมื่อ 6 มีนาคม 2561, จาก https://www.thaicert.or.th/statistics/statistics.html

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT). (2556). Digital Forensics 101 ตอนที่ 1 .สืบค้นเมื่อ 6 มีนาคม 2561, จาก https://www.thaicert.or.th/papers/general/2013/pa2013ge012.html

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT). (2556). Digital Forensics 101 ตอนที่ 2. สืบค้นเมื่อ 6 มีนาคม 2561, จาก https://www.thaicert.or.th/papers/general/2013/pa2013ge014.html

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT). (2560). ระวังภัย มัลแวร์เรียกค่าไถ่ WannaCry สืบค้นเมื่อ 6 มีนาคม 2561, จาก https://www.thaicert.or.th/alerts/user/2017/al2017us001.html#1

Chris Kim.(2012). Computer Crimes. American Criminal Law Review Volume:49 Issue:2

MGROnline.(2560). ไซแมนเทคเปิดเผยรายงานภัยคุกคามด้านความปลอดภัยบนอินเทอร์เน็ต. สืบค้นเมื่อ 4 พ.ค.2560, จาก https://mgronline.com/cyberbiz/detail/9600000045059