

บทที่ 6

จริยธรรมและความปลอดภัย

ของสารสนเทศ

01

จริยธรรมทางคอมพิวเตอร์

จริยธรรม (Ethics) หมายถึง แนวทางประพฤติปฏิบัติของคนในสังคมหนึ่ง ๆ ซึ่งเป็นมาตรฐานของสังคมนั้น ๆ ว่าเป็นคนประพฤติดีหรือชั่ว ถูกหรือผิด ควรทำหรือไม่ควรทำเป็นหลักเกณฑ์ที่ประชาชนตกลงร่วมกันเพื่อใช้เป็นแนวทางในการประพฤติปฏิบัติร่วมกันในสังคม

จริยธรรมทางคอมพิวเตอร์ หมายถึง แนวทางการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศอย่างมีศีลธรรม มีความรู้สึกผิดชอบชั่วดี หรือใช้งานในสิ่งที่ไม่บุคคลในสังคมยอมรับ ไม่ทำให้เกิดความวุ่นวายในสังคม

การที่จะระบุว่าการกระทำสิ่งใดผิดจริยธรรมนั้นอาจกล่าวได้ไม่ชัดเจนมากนัก ทั้งนี้ขึ้นอยู่กับวัฒนธรรมของสังคมในแต่ละประเทศนั้น ๆ ด้วย

ตัวอย่างของการกระทำที่ยอมรับกันโดยทั่วไป ว่าเป็นการกระทำที่ผิดจริยธรรมในการใช้งานคอมพิวเตอร์คือ ใช้ทำร้ายผู้อื่นให้เกิดความเสียหาย หรือก่อความรำคาญ

เช่น การใช้คอมพิวเตอร์และ เทคโนโลยีสารสนเทศในการขโมยข้อมูลของผู้อื่น การนำภาพหรือข้อมูลส่วนตัวของบุคคลไปลงบนอินเทอร์เน็ตโดยไม่ได้รับอนุญาต การเข้าถึงข้อมูลหรือคอมพิวเตอร์ของบุคคลอื่นโดยไม่ได้รับอนุญาต การละเมิดลิขสิทธิ์ซอฟต์แวร์ เป็นต้น

จริยธรรมเกี่ยวกับการใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศ มักจะกล่าวถึงใน
4 ประเด็นดังต่อไปนี้

01

ความเป็นส่วนตัว (Privacy)

02

ความถูกต้อง (Accuracy)

03

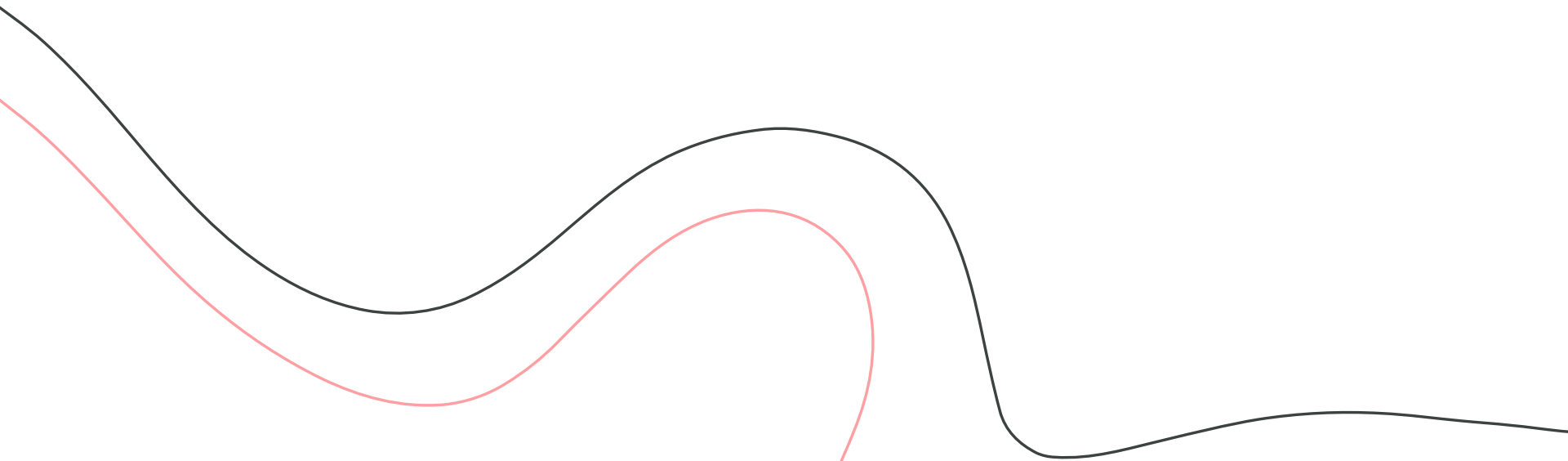
ความเป็นเจ้าของ (Intellectual Property)

04

การเข้าถึงข้อมูล (Data Accessibility)

01 ความเป็นส่วนตัว (Privacy)

ความเป็นส่วนตัวของข้อมูลและสารสนเทศ โดยทั่วไปหมายถึง สิทธิที่จะอยู่ตามลำพังและเป็นสิทธิที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น สิทธินี้ได้ครอบคลุมทั้งปัจเจกบุคคล กลุ่มคน และองค์การต่าง ๆ



ตัวอย่างการละเมิดความเป็นส่วนตัว (Privacy)

ตัวอย่างที่ 1

การเข้าไปดูข้อความในอีเมลและการบันทึกข้อมูลในเครื่องคอมพิวเตอร์ รวมทั้งการบันทึก แลกเปลี่ยนข้อมูลที่บุคคลเข้าไปใช้บริการเว็บไซต์และกลุ่มข่าวสาร การใช้เทคโนโลยีในการติดตามความ เคลื่อนไหวหรือพฤติกรรมของบุคคล

เช่น บริษัทใช้คอมพิวเตอร์และกล้องวงจรปิดในการตรวจจับหรือเฝ้าดูการปฏิบัติงานหรือการ ให้บริการของพนักงาน ถึงแม้ว่าจะเป็นการติดตามการทำงานเพื่อการพัฒนาคุณภาพการให้บริการ แต่กิจกรรม หลายอย่างของพนักงานก็ถูกเฝ้าดูด้วย พนักงานสูญเสียความเป็นส่วนตัวซึ่งการกระทำเช่นนี้ถือเป็นการผิด จริยธรรม



ตัวอย่างที่ 2

การใช้ข้อมูลของลูกค้าจากแหล่งต่าง ๆ เพื่อประโยชน์ในการขยายตลาด

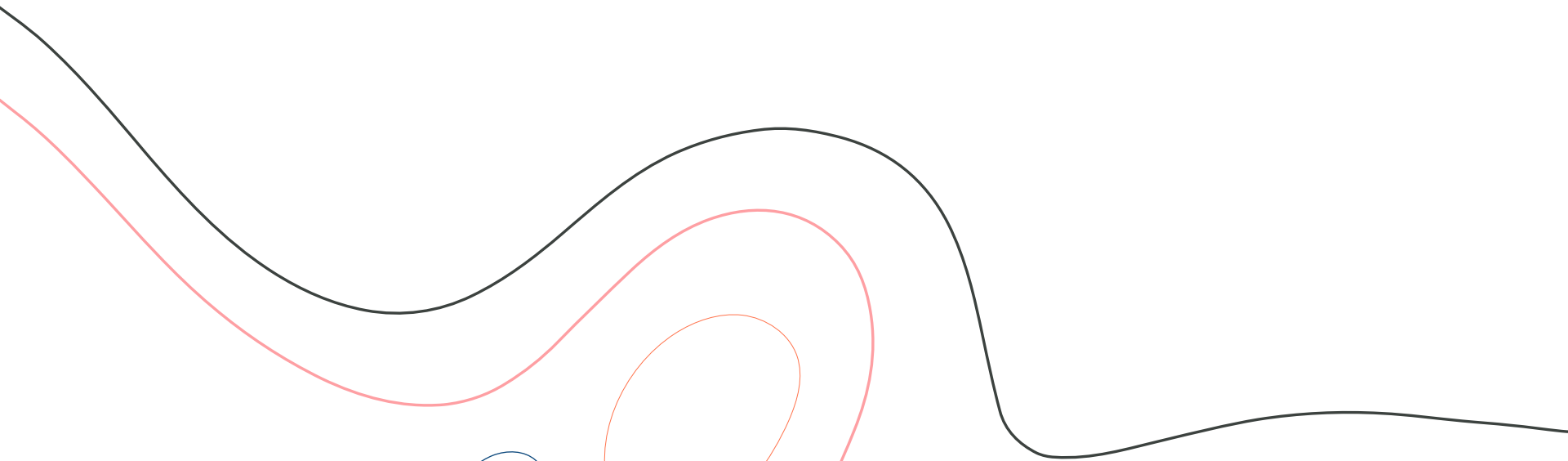
ตัวอย่างที่ 3

การรวบรวมหมายเลขโทรศัพท์ ที่อยู่อีเมล หมายเลขบัตรเครดิต และข้อมูลส่วนบุคคลอื่น ๆ เพื่อนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่ แล้วนำไปขายให้กับบริษัทอื่น



02 ความถูกต้อง (Accuracy)

ประเด็นด้านจริยธรรมที่เกี่ยวข้องกับความถูกต้องของข้อมูล โดยทั่วไปจะพิจารณาว่าใครจะเป็นผู้รับผิดชอบความถูกต้องของข้อมูลที่จัดเก็บและเผยแพร่



03

ความเป็นเจ้าของ (Intellectual Property)

สิทธิความเป็นเจ้าของ หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สิน ซึ่งอาจเป็นทรัพย์สินทั่วไปที่จับต้องได้ เช่น คอมพิวเตอร์ โทรศัพท์มือถือ รถยนต์ หรืออาจเป็นทรัพย์สินทางปัญญา (ความคิด) ที่จับต้องไม่ได้ เช่น โปรแกรมคอมพิวเตอร์ บทเพลง แต่สามารถถ่ายทอดและบันทึกลงสื่อต่าง ๆ ได้ เช่น สื่อสิ่งพิมพ์ ซีดีรอม ดีวีดีรอม ฮาร์ดดิสก์ เป็นต้น

ทรัพย์สินทางปัญญา อาจคิด หรือสร้าง หรือผลิตขึ้นจากบุคคลหรือองค์การ ซึ่งทรัพย์สินเหล่านั้นจะได้รับการคุ้มครองสิทธิภายใต้กฎหมาย ได้แก่

การคุ้มครองทรัพย์สินทางปัญญา



ความลับทางการค้า
(Trade secret)



ลิขสิทธิ์
(Copyright)



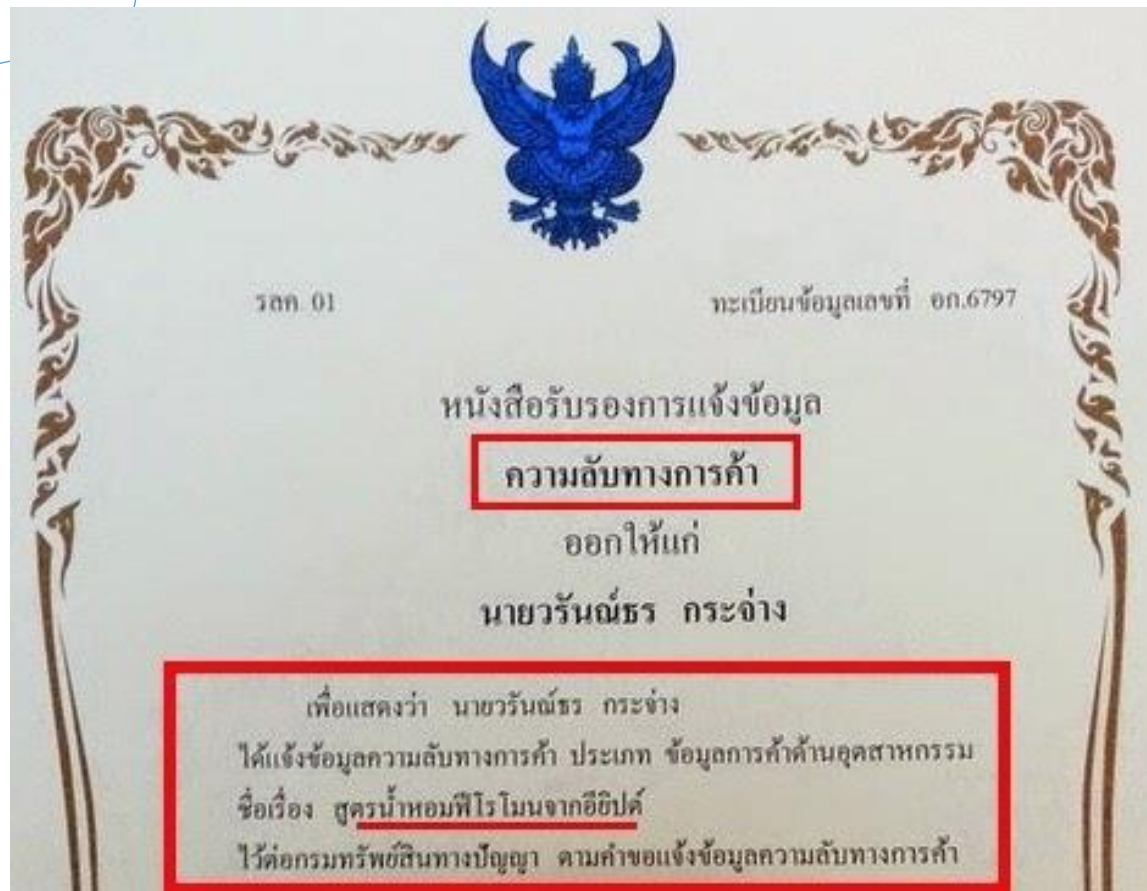
สิทธิบัตร
(Patent)

ความลับทางการค้า (Trade secret)

คือ ข้อมูลการค้าซึ่งยังไม่รู้จักกันโดยทั่วไปและมีประโยชน์ในเชิงพาณิชย์ เป็นข้อมูลต่าง ๆ ที่เกิดจากความคิดของบุคคลหรือกลุ่มบุคคลเกี่ยวกับข้อมูลการค้า สูตร โปรแกรม วิธีการเทคนิคหรือกรรมวิธีต่าง ๆ เช่น สูตรยา สูตรอาหาร สูตรเครื่องดื่ม สูตรเครื่องสำอาง กรรมวิธีการผลิต บัญชีรายชื่อลูกค้า ข้อมูลการบริหารธุรกิจ กลยุทธ์การโฆษณาสินค้า เป็นต้น

ผู้ที่เป็นเจ้าของความลับทางการค้าจะได้รับความคุ้มครองตลอดไปตราบเท่าที่ความลับทางการค้านั้นยังคงเป็นความลับอยู่

การละเมิดสิทธิในความลับทางการค้า ได้แก่ การกระทำที่เป็นการเปิดเผย เอาไป หรือใช้ซึ่งความลับทางการค้า โดยไม่ได้รับความยินยอมจากเจ้าของความลับทางการค้านั้น



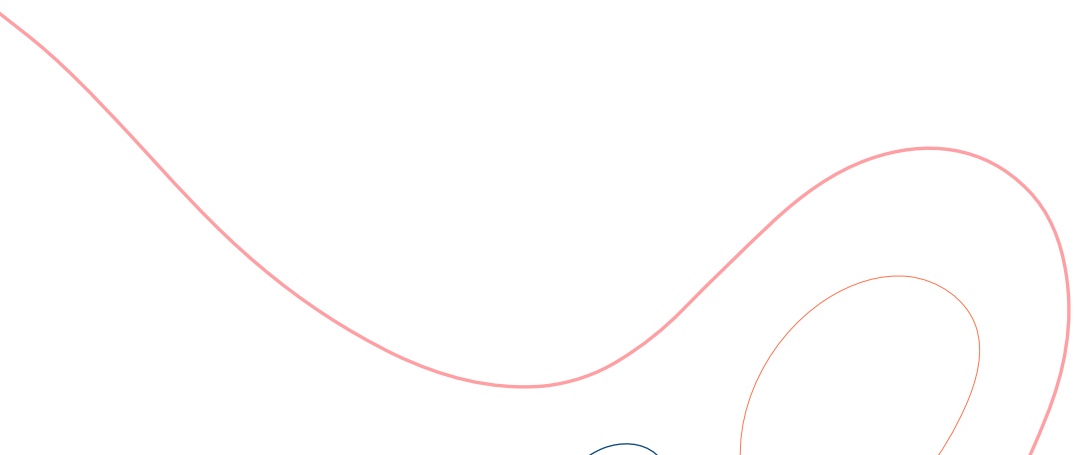
ตัวอย่างหนังสือรับรองความลับทางการค้า



ลิขสิทธิ์ (Copyright)

เป็นสิทธิในการกระทำใด ๆ (ตีพิมพ์ แสดงผลงาน หรือแจกจ่ายผลงาน) **เกี่ยวกับงานที่สร้างสรรค์ขึ้น** โดยใช้สติปัญญาความรู้ ความสามารถ โดยไม่ลอกเลียนงานของผู้อื่น

ซึ่งเป็นสิทธิที่ได้รับการคุ้มครองในการคัดลอกหรือทำซ้ำผลงาน ถึงแม้ว่าผลงานนั้นจะนำเสนอทางอินเทอร์เน็ต และตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 **จะคุ้มครองผลงานนั้น ๆ เป็นเวลา 50 ปี** หลังจากที่ยานได้คิดค้นขึ้น หรือตั้งแต่ที่มีการแสดงผลงานเป็นครั้งแรก



ลิขสิทธิ์ (Copyright) กฎหมายที่คุ้มครองลิขสิทธิ์ แบ่งงานที่สร้างสรรค์ทั้งหมด 9 ประเภท คือ

- 1) งานวรรณกรรม (หนังสือ จุลสาร สิ่งพิมพ์ โปรแกรมคอมพิวเตอร์ ฯลฯ)
- 2) งานนาฏกรรม (ท่าเต้น ท่ารำ ฯลฯ)
- 3) งานศิลปกรรม (จิตรกรรม ประติมากรรม ภาพพิมพ์ ภาพถ่าย ศิลปประยุกต์ ฯลฯ)
- 4) งานดนตรีกรรม (ทำนอง ทำนองและเนื้อร้อง ฯลฯ)
- 5) งานสิ่งบันทึกเสียง (เทป ซีดี)
- 6) งานโสตทัศนวัสดุ (วีซีดี ดีวีดี ที่มีภาพหรือมีทั้งภาพและเสียง)
- 7) งานภาพยนตร์
- 8) งานแพร่เสียงแพร่ภาพ
- 9) งานอื่นใดในแผนกวรรณคดี วิทยาศาสตร์ หรือศิลปะ

รทช.01 ทะเบียนข้อมูลเลขที่ ว. 1878

หนังสือรับรองการแจ้งข้อมูล
ลิขสิทธิ์
ออกให้เพื่อแสดงว่า
ห้างหุ้นส่วนจำกัด แอคกรีท

ได้แจ้งข้อมูลลิขสิทธิ์ ประเภทงาน วรรณกรรม
ลักษณะงาน โปรแกรมคอมพิวเตอร์
ชื่อผลงาน โปรแกรม WISP-Management วิศวกรรมทรัพย์สินทางปัญญา
ตามคำขอแจ้งข้อมูลลิขสิทธิ์ เลขที่ 108210 เมื่อวันที่ 12 เดือน กันยายน พ.ศ. 2548

ให้ไว้ ณ วันที่ 4 เดือน ตุลาคม พ.ศ. 2548

ลงชื่อ (นางสุจินดา กุญชรินทร์)
เจ้าหน้าที่วิศวกรรมทะเบียนการค้า 7
ปฏิบัติราชการแทนผู้อำนวยการสำนักลิขสิทธิ์

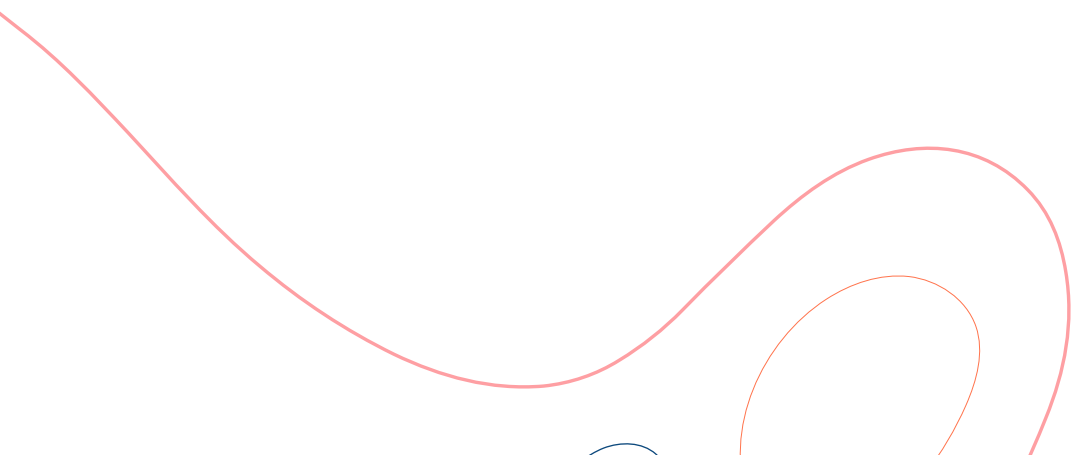
หมายเหตุ
การเปลี่ยนแปลงรายการข้างต้น ให้ดูวันหลัง

ตัวอย่างหนังสือรับรองลิขสิทธิ์



สิทธิบัตร (Patent)

เป็นหนังสือสำคัญที่ออกรับรองให้เพื่อกู้มครองการประดิษฐ์ หรือออกแบบผลิตภัณฑ์ต่าง ๆ ซึ่ง
พระราชบัญญัติสิทธิบัตร พ.ศ. 2522 จะคุ้มครองสิทธิบัตรที่แจ้งจด 20 ปี นับตั้งแต่วันขอรับสิทธิบัตร





อนุสิทธิบัตร

อาศัยอำนาจตามความในพระราชบัญญัติสิทธิบัตร พ.ศ. 2522
แก้ไขเพิ่มเติมโดยพระราชบัญญัติสิทธิบัตร (ฉบับที่ 3) พ.ศ. 2542
อธิบดีกรมทรัพย์สินทางปัญญาออกอนุสิทธิบัตรฉบับนี้ให้แก่

มหาวิทยาลัยสวนดุสิต

สำหรับการประดิษฐ์ตามรายละเอียดการประดิษฐ์ ข้อถ้อยสิทธิ และรูปเขียน (ถ้ามี)
ตามกฎหมายในอนุสิทธิบัตรนี้

เลขที่คำขอ 1503000437

ออกบัตรอนุสิทธิบัตร 27 มีนาคม 2558

ประดิษฐ์ นางสาวจิราภรณ์ ทองต้น และคณะ

แสดงถึงการประดิษฐ์ เครื่องหาตำแหน่งดาวเทียมที่มีสารสกัดจากโกล

ให้ผู้ทรงอนุสิทธิบัตรและหน้าที่ตามกฎหมายว่าด้วยสิทธิบัตรทุกประการ

ออกให้ ณ วันที่ 1 เดือน มิถุนายน พ.ศ. 2560

หมดอายุ ณ วันที่ 26 เดือน มีนาคม พ.ศ. 2564

(ลงชื่อ).....

ผู้ลงนามในสัญญา น.โควณชีวีต

รองอธิบดีกรมทรัพย์สินทางปัญญา ปฏิบัติราชการแทน

อธิบดีกรมทรัพย์สินทางปัญญา

ผู้อำนวยการบริหาร

๒๕๖๐

พนักงานเจ้าหน้าที่

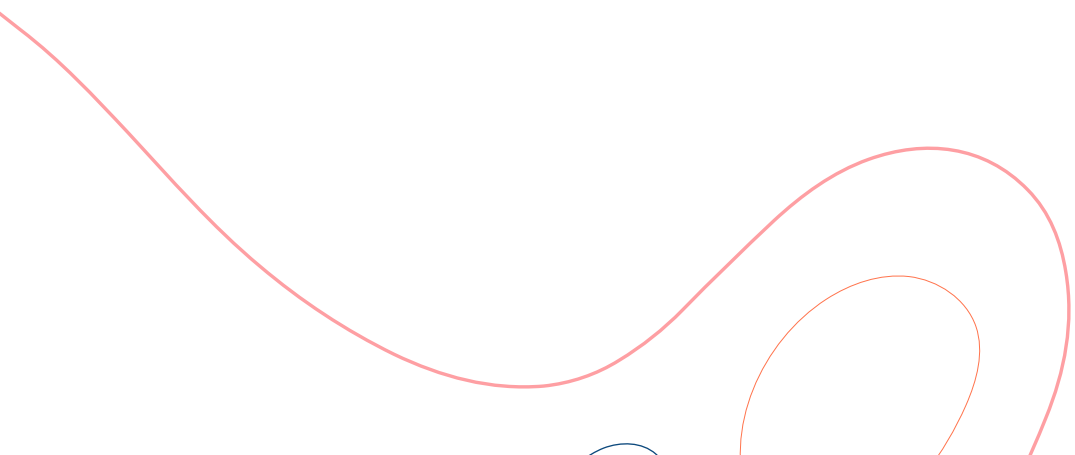
หมายเหตุ

1. ผู้ทรงอนุสิทธิบัตรต้องชำระค่าธรรมเนียมรายปีเริ่มตั้งแต่ปีที่ 5 ของอายุสิทธิบัตร มิฉะนั้น อนุสิทธิบัตรจะสิ้นสุดอายุ
2. ผู้ทรงอนุสิทธิบัตรจะขอชำระค่าธรรมเนียมรายปีล่วงหน้าโดยชำระทั้งหมดในคราวเดียวกันได้
3. ภายใน 90 วันก่อนวันสิ้นสุดอนุสิทธิบัตร ผู้ทรงอนุสิทธิบัตรมีสิทธิขอต่ออายุอนุสิทธิบัตรได้ 2 ครั้ง มีกำหนดคราวละ 2 ปี โดยยื่นคำขอต่ออายุ ต่อพนักงานเจ้าหน้าที่
4. การอนุญาตให้ใช้สิทธิในอนุสิทธิบัตรและการโอนอนุสิทธิบัตรต้องทำเป็นหนังสือและจดทะเบียนต่อพนักงานเจ้าหน้าที่

029346

ความลับทางการค้า ลิขสิทธิ์ และสิทธิบัตร แตกต่างกันตรงที่ ผลงานที่ได้รับความคุ้มครองจาก
ลิขสิทธิ์และสิทธิบัตรเป็นสิ่งที่เปิดเผยต่อสาธารณะ เพราะสร้างขึ้นเพื่อให้คนทั่วไปใช้

และโปรแกรมคอมพิวเตอร์จะได้รับความคุ้มครองภายใต้กฎหมายลิขสิทธิ์เนื่องจากถูกจัดอยู่ใน
ประเภทเดียวกับงานเขียน

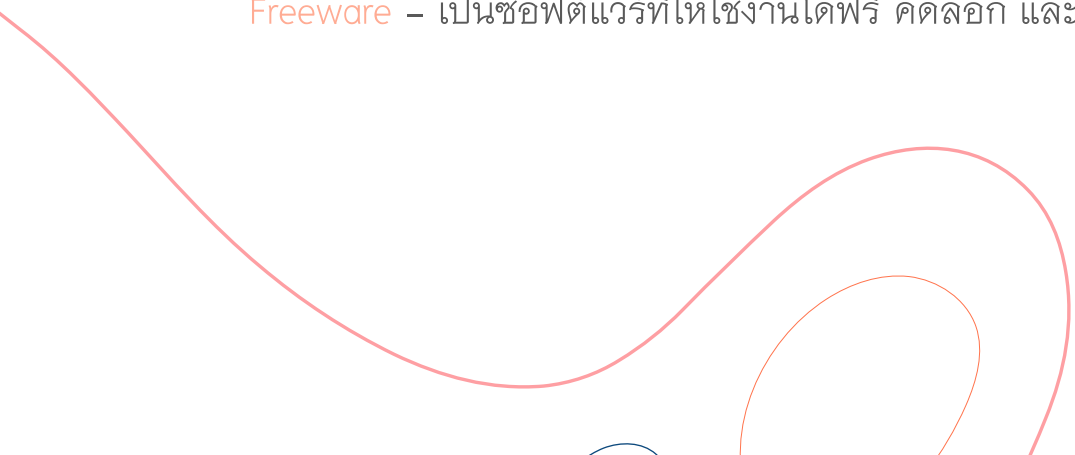


การคัดลอกโปรแกรมคอมพิวเตอร์ให้กับบุคคลอื่น เป็นการกระทำที่จะต้องพิจารณาให้รอบคอบก่อนว่าโปรแกรมที่จะทำการคัดลอกนั้นเป็นโปรแกรมคอมพิวเตอร์ที่ผู้ใช้มีสิทธิในระดับใด ตัวอย่างเช่น

Copyright software – เป็นซอฟต์แวร์ลิขสิทธิ์ ที่ผู้ใช้ซื้อลิขสิทธิ์มา และมีสิทธิใช้

Shareware – เป็นซอฟต์แวร์ที่ให้ทดลองใช้ได้ ก่อนที่จะตัดสินใจซื้อ

Freeware – เป็นซอฟต์แวร์ที่ให้ใช้งานได้ฟรี คัดลอก และเผยแพร่ให้ผู้อื่นได้



04 การเข้าถึงข้อมูล (Data Accessibility)

การเข้าใช้งานโปรแกรมหรือระบบคอมพิวเตอร์มักจะมีการกำหนดสิทธิตามระดับของผู้ใช้งาน ทั้งนี้ เพื่อเป็นการป้องกันการเข้าไปดำเนินการต่าง ๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้อง และเป็นการรักษา ความเป็นส่วนตัวของข้อมูล

ตัวอย่างสิทธิในการใช้งานระบบ เช่น การบันทึก การแก้ไข ปรับปรุง และการลบ เป็นต้น

ดังนั้นในการพัฒนาระบบคอมพิวเตอร์จึงได้มีการออกแบบระบบรักษาความปลอดภัยไว้ การเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอมนั้น ก็ถือเป็นการทำผิดจริยธรรมเช่นเดียวกับการละเมิด ข้อมูลส่วนตัว

การเข้าไปดูข้อความในอีเมลและการบันทึกข้อมูลในเครื่องคอมพิวเตอร์ของผู้อื่น โดยที่เจ้าของไม่อนุญาต เป็นการละเมิดจริยธรรมข้อใด

ความถูกต้อง

ความเป็นเจ้าของ

ความเป็นส่วนตัว

ข้อใด คือหนังสือสำคัญที่ออกรับรองให้เพื่อกู้ยืมโครงการประดิษฐ์ หรือออกแบบผลิตภัณฑ์ต่าง ๆ

ความลับทางการค้า

ลิขสิทธิ์

สิทธิบัตร

โปรแกรมคอมพิวเตอร์จะได้รับความคุ้มครองภายใต้กฎหมายใด

ความลับทางการค้า

ลิขสิทธิ์

สิทธิบัตร

การคุ้มครองทรัพย์สินทางปัญญาใด ไม่สามารถ¹สิ่ง¹ที่เปิดเผยต่อสาธารณะได้

ความลับทางการค้า

ลิขสิทธิ์

สิทธิบัตร

คุ้มครองสิทธิบัตรที่แจ้งจดทะเบียนเวลากี่ปี

20 ปี

ตลอดไป

50 ปี

ลิขสิทธิ์ (Copyright) จะคุ้มครองผลงานนั้น ๆ เป็นเวลาที่กี่ปี หลังจากทำงานได้คิดค้นขึ้น หรือตั้งแต่ที่มีการ
แสดงผลงานเป็นครั้งแรก

20 ปี

ตลอดไป

50 ปี

เป็นซอฟต์แวร์ที่ให้ทดลองใช้ได้ ก่อนที่จะตัดสินใจซื้อ หมายถึง ข้อใด

Copyright software

Shareware

Freeware

02

อาชญากรรมทางคอมพิวเตอร์

อาชญากรรมทางคอมพิวเตอร์ (Computer crime) หรืออาชญากรรมไซเบอร์ (Cyber crime) เป็นการกระทำที่ผิดกฎหมายโดยใช้คอมพิวเตอร์และเทคโนโลยีสารสนเทศเป็นเครื่องมือ

เช่น การโจรกรรมข้อมูลหรือความลับของบริษัทคู่แข่ง การบิดเบือนข้อมูล การฉ้อโกง การหลอกลวง การฟอกเงิน การถอดรหัสโปรแกรมคอมพิวเตอร์ ไวรัสคอมพิวเตอร์ การทำลายข้อมูลและระบบ การป้องกันในระบบเครือข่าย การก่อกรวนโดยกลุ่มแฮกเกอร์ (Hacker) รวมไปถึง การก่อการร้ายในโลกไซเบอร์ (Cyber terrorist) เป็นต้น

แฮกเกอร์ หรือนักเลงคอมพิวเตอร์ คือ บุคคลที่มีความรู้ในระบบคอมพิวเตอร์เป็นอย่างดี สามารถเข้าไปถึงข้อมูลในคอมพิวเตอร์ โดยเจาะผ่านระบบรักษาความปลอดภัยของคอมพิวเตอร์

ซึ่งเป็นการใช้ความรู้ความสามารถในทางที่ไม่ถูกต้อง เช่น การลักลอบเข้าไปยังคอมพิวเตอร์เครื่องอื่นผ่านการสื่อสารบนระบบเครือข่าย โดยไม่ได้รับอนุญาต

อาจจะมีวัตถุประสงค์เข้าไปเพื่อหาช่องโหว่ของระบบเครือข่าย หรืออาจกระทำไปด้วยความสนุก ต้องการทดสอบความสามารถของตนเอง รวมถึงการวัดความสามารถกับเพื่อน ๆ

แครกเกอร์ (Cracker) หรือนักเจาะระบบ คือแฮกเกอร์ที่มีความชำนาญทางด้านคอมพิวเตอร์ ระบบเครือข่าย หรือการเขียนโปรแกรมคอมพิวเตอร์มากเป็นพิเศษ ลักลอบเข้าไปยังคอมพิวเตอร์ของผู้อื่น**เพื่่อมุ่งทำลายระบบ** เจาะระบบเพื่อล้วงข้อมูล คัดลอก เปลี่ยนแปลง ลบ หรือทำลายข้อมูลให้เสียหาย จะสร้างความเสียหายที่รุนแรง เพื่อประโยชน์ของตนเองหรือพวกพ้อง

แครกเกอร์จะสร้างความเสียหายที่ร้ายแรงกว่าแฮกเกอร์มาก การกระทำของแฮกเกอร์หรือแครกเกอร์ เป็นการกระทำที่ผิดกฎหมายทั้งสิ้น

การใช้คอมพิวเตอร์ในฐานะ “เป็นเครื่องมือในการก่ออาชญากรรม”

01

การขโมยหมายเลขบัตรเครดิต
(Credit card theft)

02

การแอบอ้างตัว (Identity theft)

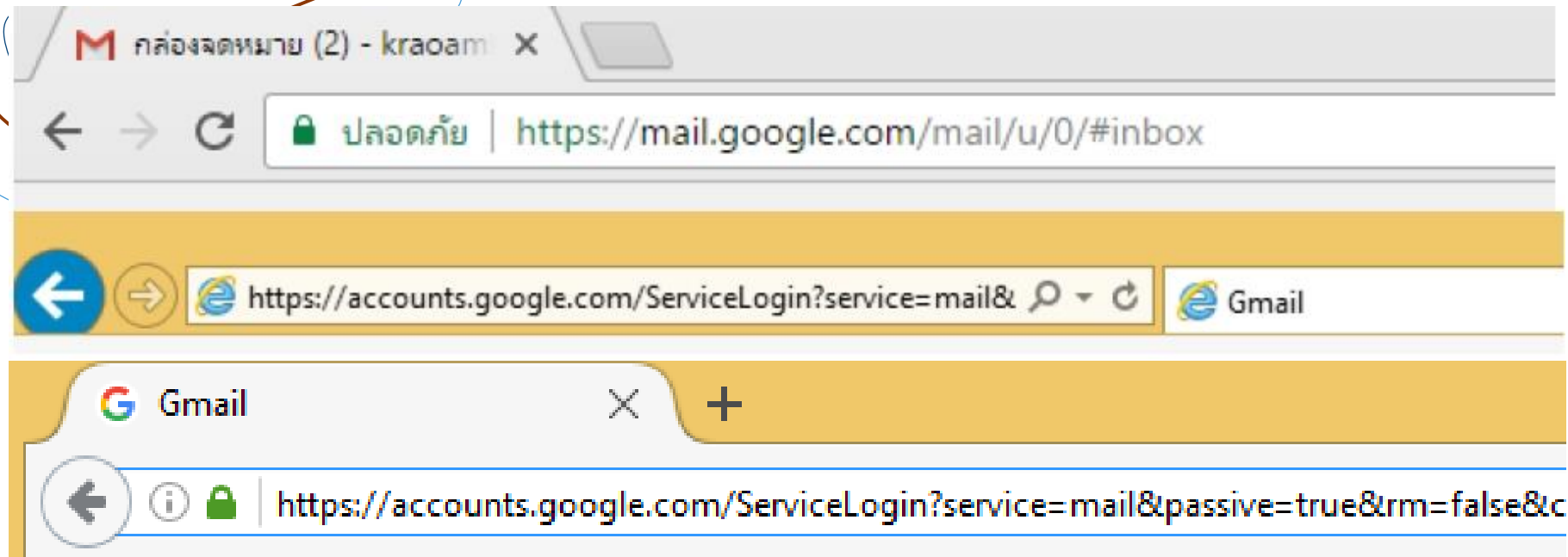
03

การสแกมทางคอมพิวเตอร์ (Scam)

01 การขโมยหมายเลขบัตรเครดิต (Credit card theft)

หากบัตรเครดิตหาย จะด้วยทำหายเองหรือถูกขโมยก็ตาม เมื่อเจ้าของบัตรรู้ต้องรีบแจ้งระงับการใช้บัตรในทันที แต่ถ้าถูกขโมยหมายเลขบัตรเครดิตทางอิเล็กทรอนิกส์แล้ว เป็นการยากที่เจ้าของจะรู้จนกว่าจะได้รับใบแจ้งยอดการใช้เงินจากบัตรนั้น ในบางครั้งขโมยอาจนำหมายเลขบัตรไปใช้สำหรับการเข้าฐานข้อมูลเครดิต และบัญชีธนาคาร เพื่อจะกระทำการอื่น ๆ ต่อไป

ดังนั้นเมื่อจะซื้อสินค้าและชำระเงินด้วยบัตรเครดิตผ่านทางอินเทอร์เน็ตจะต้องแน่ใจว่าระบบมีการรักษาความปลอดภัย เช่น ถ้าทำธุรกรรมผ่านเว็บไซต์หรือกำลังใช้เว็บไซต์ ให้สังเกตว่าที่ Address bar ของ Web browser จะมีรูปแม่กุญแจล็อกอยู่ และที่อยู่เว็บไซต์หรือ URL จะระบุ https://



สัญลักษณ์รูปแม่กุญแจล็อก
หรือ https:// ปรากฏอยู่ที่แอดเดรสบาร์ของเว็บเบราว์เซอร์

02 การแอบอ้างตัว (Identity theft)

เป็นการแอบอ้างตัวของผู้กระทำต่อบุคคลที่สามว่าตนเป็นอีกคนหนึ่ง การกระทำในลักษณะนี้ จะใช้ลักษณะเฉพาะตัว ได้แก่ หมายเลขบัตรประชาชน หมายเลขบัตรเครดิต หนังสือเดินทาง และข้อมูลส่วนบุคคลอื่น ๆ ของผู้ถูกกระทำหรือเอื้อไปใช้แอบอ้างเพื่อหาผลประโยชน์

ตัวอย่างเช่น นายดำแอบอ้างตัวว่าเป็นนายแดง โดยการส่งอีเมลล์และเอกสารปลอมที่แสดงตนว่าเป็นนายแดงจริง เพื่อขอเปลี่ยนแปลงเจ้าของเว็บไซต์จากนายแดงเป็นนายดำ ดังนั้นนาย ดำก็จะได้รับผลประโยชน์ต่าง ๆ โดยที่ไม่ต้องจ่ายค่าสิทธิในการใช้ที่อยู่อินเทอร์เน็ตนั้น

03 การเล่นเกมทางคอมพิวเตอร์ (Scam)

เป็นการกระทำโดยใช้คอมพิวเตอร์เป็นเครื่องมือในการหลอกลวงผู้อื่น ปัจจุบันมีรูปแบบที่แตกต่างกันมากมาย เช่น

1) การส่งข้อความ หรือโฆษณาบนเว็บไซต์ว่าผู้ใช้สามารถเดินทางเข้าพักหรือท่องเที่ยวแบบหรูในราคาถูก แต่เมื่อเข้าไปใช้บริการจริง กลับไม่เป็นอย่างที่บอกไว้ หรือบางครั้งอาจต้องมีการจ่ายเพิ่มเติม ซึ่งไม่ได้แจ้งไว้ล่วงหน้า ดังนั้นหากเกิดกรณีเช่นนี้ ก่อนตัดสินใจควรจะต้องมีข้อตกลงเป็นลายลักษณ์อักษร รวมทั้งข้อตกลงเกี่ยวกับการยกเลิกสัญญาให้ชัดเจนเสียก่อน

2) การเสนอให้ผู้ใช้สามารถเข้าไปใช้บริการเว็บไซต์เฉพาะผู้ใหญ่ได้ฟรี หากผู้ใช้ระบุหมายเลขบัตรเครดิตเพื่อเป็นการยืนยันอายุของผู้ใช้ หลังจากนั้นผู้ใช้ก็จะได้รับใบเรียกเก็บเงินจากบัตรเครดิตโดยที่ผู้ใช้ไม่ได้ซื้อสินค้าหรือรับบริการใด ๆ เลย ดังนั้นก่อนที่ผู้ใช้จะกรอกหมายเลขบัตรเครดิตจะต้องอ่านรายละเอียดหรือข้อตกลงให้รอบคอบเสียก่อน

คอมพิวเตอร์ในฐานะ “เป็นเป้าหมายของอาชญากรรม”

01

การเข้าถึงและการใช้คอมพิวเตอร์
โดยไม่ได้รับอนุญาต

02

การก่อกวนหรือการทำลายข้อมูล

03

การทำให้ระบบปฏิเสธการให้บริการ
(Denial of Service)

04

การขโมยคอมพิวเตอร์

01 การเข้าถึงและการใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาต

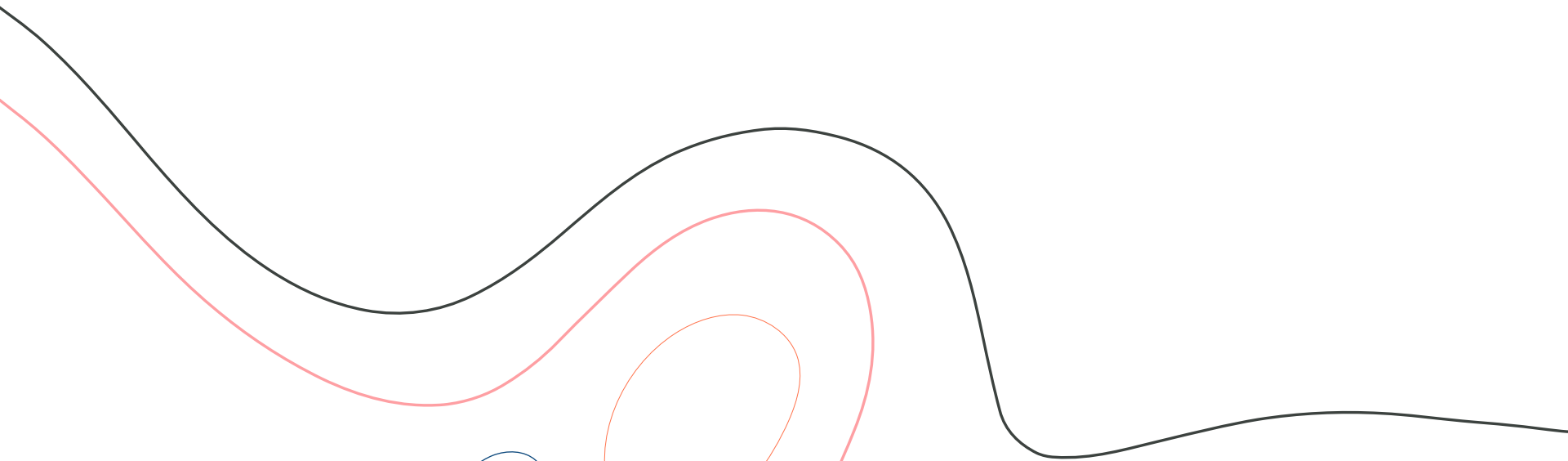
เป็นการกระทำต่าง ๆ ที่เกี่ยวข้องกับคอมพิวเตอร์หรือข้อมูลของผู้อื่นโดยที่เจ้าของไม่อนุญาต การเข้าถึงอาจใช้วิธีขโมยรหัสส่วนตัว (Personal identification number : PIN)* หรือการเข้ารหัสผ่าน (Password) ซึ่งการกระทำโดยมิชอบนี้อาจก่อให้เกิดความเสียหายแก่บุคคลหรือองค์กร

PIN – Personal Identification Number* คือเลขรหัสลับที่ใช้ระหว่างระบบและผู้ใช้งาน เพื่อใช้ในการยืนยันตัวตนเข้าสู่ระบบ ส่วนใหญ่จะต้องใช้คู่กับ Identification ที่ไม่ลับด้วย เช่น ชื่อลูกค้า หมายเลขบัตรเครดิต หรือ username ดังนั้นมีเพียงแค่ PIN อย่างเดียวจะไม่เพียงพอให้เข้าสู่ระบบได้

02 การก่อกวนหรือการทำลายข้อมูล

ผู้ใช้สามารถที่จะตกเป็นเหยื่อของการถูกขโมยข้อมูลได้เนื่องจากบางบริษัทต้องการนำข้อมูลนั้น ๆ เพื่อใช้ในการแข่งขันทางธุรกิจ

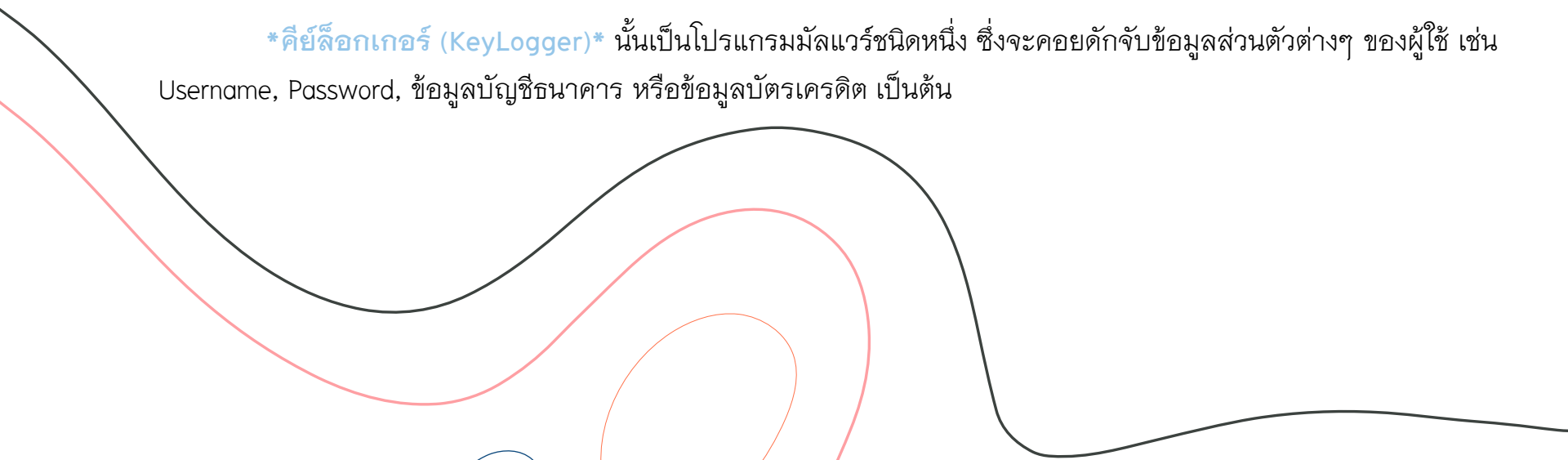
การขโมยข้อมูลจะเกี่ยวข้องกับอาชญากรรมประเภทอื่น ๆ เช่น การเข้าถึงข้อมูลหรือเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต เป็นต้น

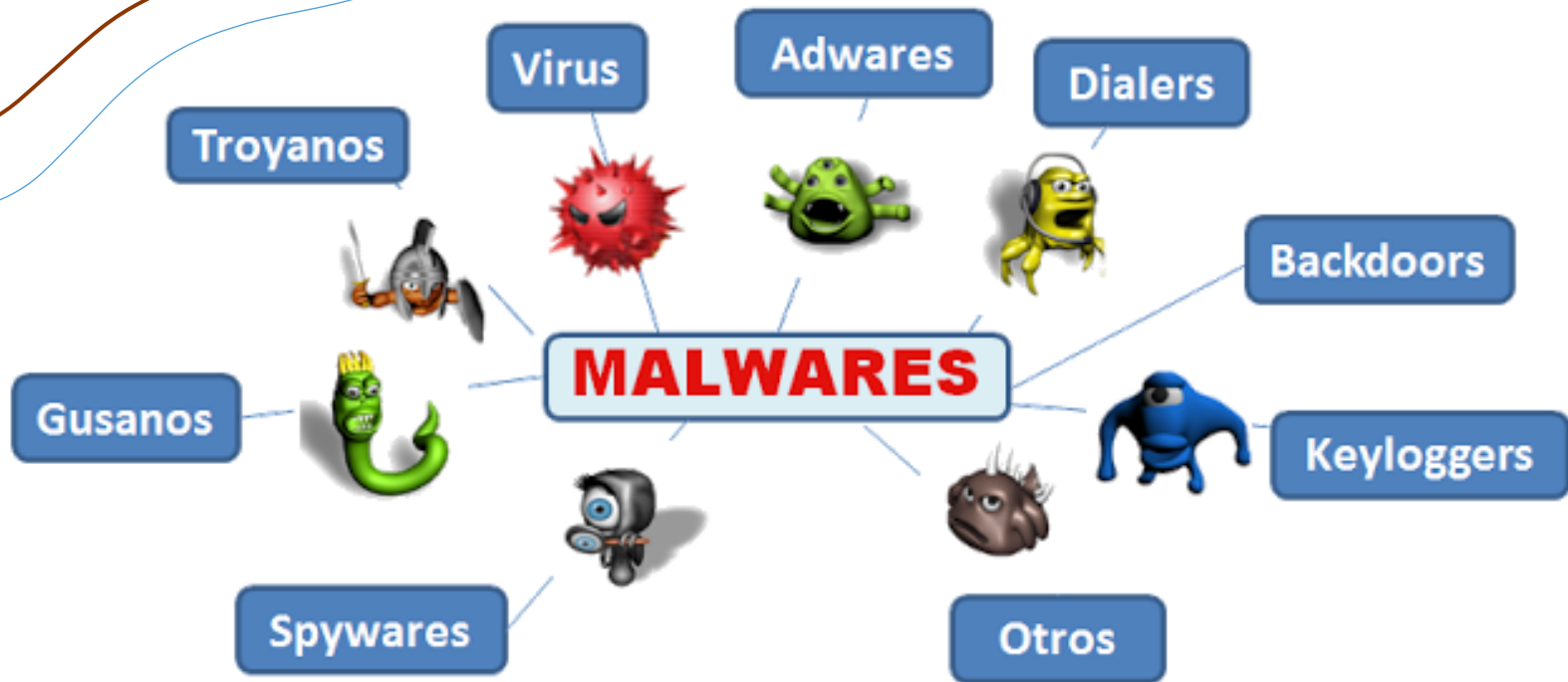


มัลแวร์ (Malware) ย่อมาจากคำว่า Malicious Software หมายถึงโปรแกรมประสงค์ร้ายต่าง ๆ โดยทำงานในลักษณะที่เป็นการโจมตีระบบ การทำให้ระบบเสียหาย รวมไปถึงการโจรกรรมข้อมูล

มัลแวร์ แบ่งออกได้หลากหลายประเภท อาทิเช่น ไวรัส (Virus) เวิร์ม (Worm) หรือหนอนอินเทอร์เน็ต ม้าโทรจัน (Trojan Horse) การแอบดักจับข้อมูล (Spyware) คีย์ล็อกเกอร์ (Key Logger)* บนเครื่องคอมพิวเตอร์ของผู้ใช้งาน

คีย์ล็อกเกอร์ (KeyLogger) นั้นเป็นโปรแกรมมัลแวร์ชนิดหนึ่ง ซึ่งจะคอยดักจับข้อมูลส่วนตัวต่างๆ ของผู้ใช้ เช่น Username, Password, ข้อมูลบัญชีธนาคาร หรือข้อมูลบัตรเครดิต เป็นต้น





มัลแวร์ (Malware)

ประเภทของมัลแวร์ (Malware)



ไวรัสคอมพิวเตอร์ (Computer Virus)



เวิร์ม (Worm)



ม้าโทรจัน (Trojan Horse)



ข่าวหลอกลวง (Hoax)

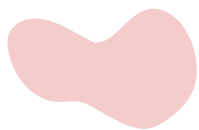


ไวรัสคอมพิวเตอร์ (Computer Virus)

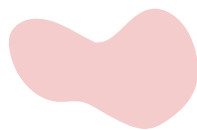
เป็นโปรแกรมที่สามารถติดต่อจากไฟล์หนึ่งไปยังอีกไฟล์หนึ่งภายในระบบเดียวกัน หรือจากคอมพิวเตอร์เครื่องหนึ่งไปยังเครื่องอื่นโดยการแนบตัวเองไปกับโปรแกรมอื่น สามารถทำลายฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูล

การสร้างความเสียหายจะแบ่งเป็น 2 ลักษณะคือ ไวรัสที่แสดงข้อความรบกวนหรือทำให้คอมพิวเตอร์ทำงานช้าลง แต่จะไม่ทำลายข้อมูล **อีกประเภทหนึ่ง** จะทำลายการทำงานของระบบคอมพิวเตอร์ ได้แก่ การลบไฟล์ การสั่งปิดเครื่องคอมพิวเตอร์ หรือการรบกวนการทำงานของโปรแกรมอื่น ๆ ที่ติดตั้งอยู่ในเครื่องที่ติดไวรัส เป็นต้น

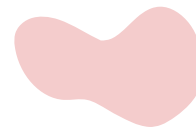
ประเภทไวรัสคอมพิวเตอร์ (Computer Virus)



ไวรัสที่ทำงานบน Boot sector



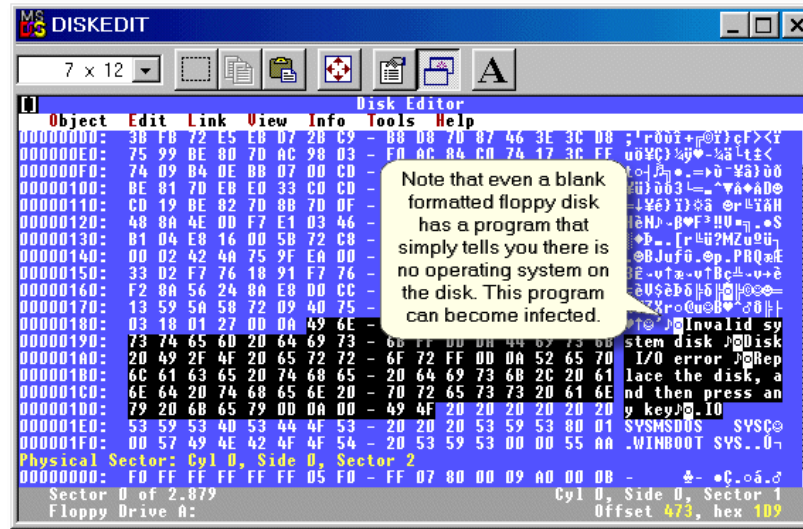
ไวรัสที่เกาะติดที่แฟ้มงานหรือ
โปรแกรม



แมโครไวรัส (Macro Virus)

ไวรัสที่ทำงานบน Boot sector

หรือบางครั้งเรียก System Virus ไวรัสประเภทนี้จะแฝงตัวอยู่ที่ Boot sector ของฮาร์ดดิสก์ แล้วยังสามารถที่จะฝังตัวอยู่ในหน่วยความจำของเครื่องคอมพิวเตอร์ได้ด้วย จะทำงานเมื่อเริ่มเปิดระบบ

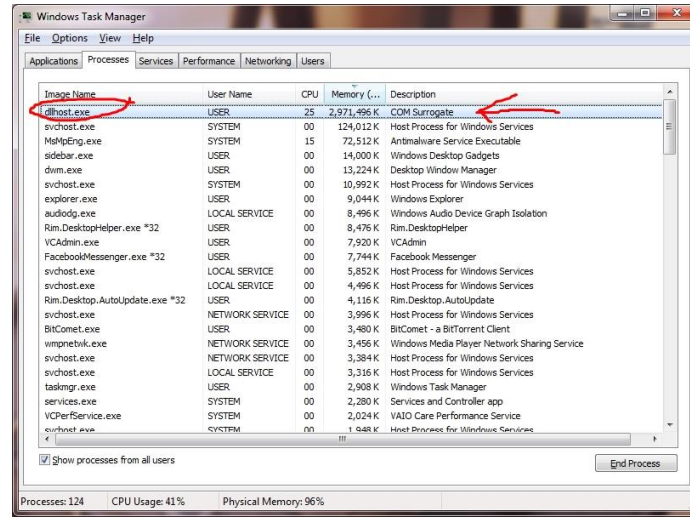


ไวรัสที่เกาะติดที่แฟ้มงานหรือโปรแกรม

ไวรัสชนิดนี้จะแฝงตัวอยู่ตามไฟล์ต่าง ๆ ส่วนใหญ่จะเป็นไฟล์ที่มีนามสกุลเป็น .exe และ .com เพราะเป็นไฟล์ที่ถูกเรียกใช้งานเป็นประจำ

การทำงานของไวรัสจะเกิดขึ้นเมื่อผู้ใช้เรียกใช้ไฟล์ที่ติดไวรัส จากนั้นไวรัสจะฝังตัวเองในหน่วยความจำของคอมพิวเตอร์

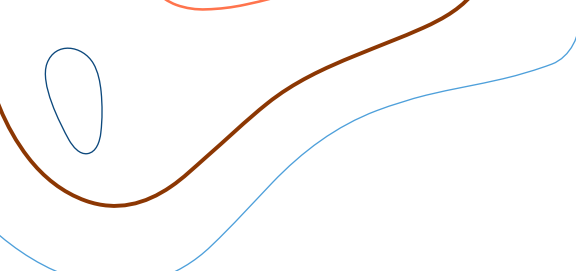
โดยปกติการติดไวรัสประเภทนี้มักมาจากการดาวน์โหลดไฟล์หรือโปรแกรมจากอินเทอร์เน็ตในแหล่งที่ไม่ปลอดภัย หรือการเปิดไฟล์ที่แนบมากับอีเมล



แมโครไวรัส (Macro Virus)

เป็นไวรัสที่ทำงานบนโปรแกรมที่ใช้ภาษาแมโคร เช่น โปรแกรมประมวลคำ (Word processing) และโปรแกรมตารางคำนวณ (Spreadsheet) เป็นต้น





มีไวรัสประเภทหนึ่งเรียกว่า **ลอจิกบอมบ์ (logic bomb)** หรือ **ระเบิดเวลา (Time bomb)** ซึ่งเป็นไวรัสที่ออกแบบมาให้ทำงานตามเงื่อนไขหรือเวลาที่กำหนดไว้ จะทำงานเมื่อนาฬิกาของเครื่องเดินถึงเวลาที่ถูกเขียนให้ไวรัสตื่นขึ้นมาทำงานนั่นเอง

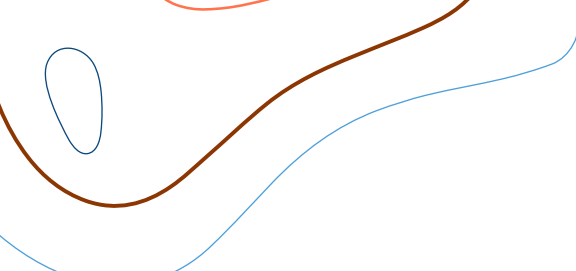
ไวรัสคอมพิวเตอร์ที่ระบาดไปทั่วโลกและมีความรุนแรงมากเป็นมัลแวร์เรียกค่าไถ่ชื่อ **วอนนา คราย (WannaCry)** โดยมัลแวร์ดังกล่าวมีจุดประสงค์หลักเพื่อเข้ารหัสลับข้อมูลในคอมพิวเตอร์เพื่อเรียกค่าไถ่ หากไม่จ่ายเงินตามที่เรียกจะไม่สามารถเปิดไฟล์ได้



เวิร์ม (Worm)

หรือหนอน คุณสมบัติพิเศษของเวิร์ม คือ สามารถแพร่กระจายตัวของมันเองได้โดยอัตโนมัติและไม่ต้องอาศัยโปรแกรมอื่นในการแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ ผ่านทางเครือข่าย

เวิร์มจะแพร่กระจายโดยการค้นหาที่อยู่อีเมลของผู้ใช้จาก E-mail Address Book จากนั้นก็จะส่งตัวมันเองไปกับอีเมลนั้น ๆ



เมื่อผู้ใช้เปิดไฟล์อ่าน เวิร์มก็จะเริ่มทำงานโดยการคัดลอกตัวเองและส่งอีเมลอิเล็กทรอนิกส์ไปยังคนอื่น ๆ ที่มีรายชื่ออยู่ใน E-mail Address Book ของผู้ใช้เหมือนกับการส่งอีเมลลูกโซ่ถึงคนอื่น ๆ ต่อไปเรื่อย ๆ

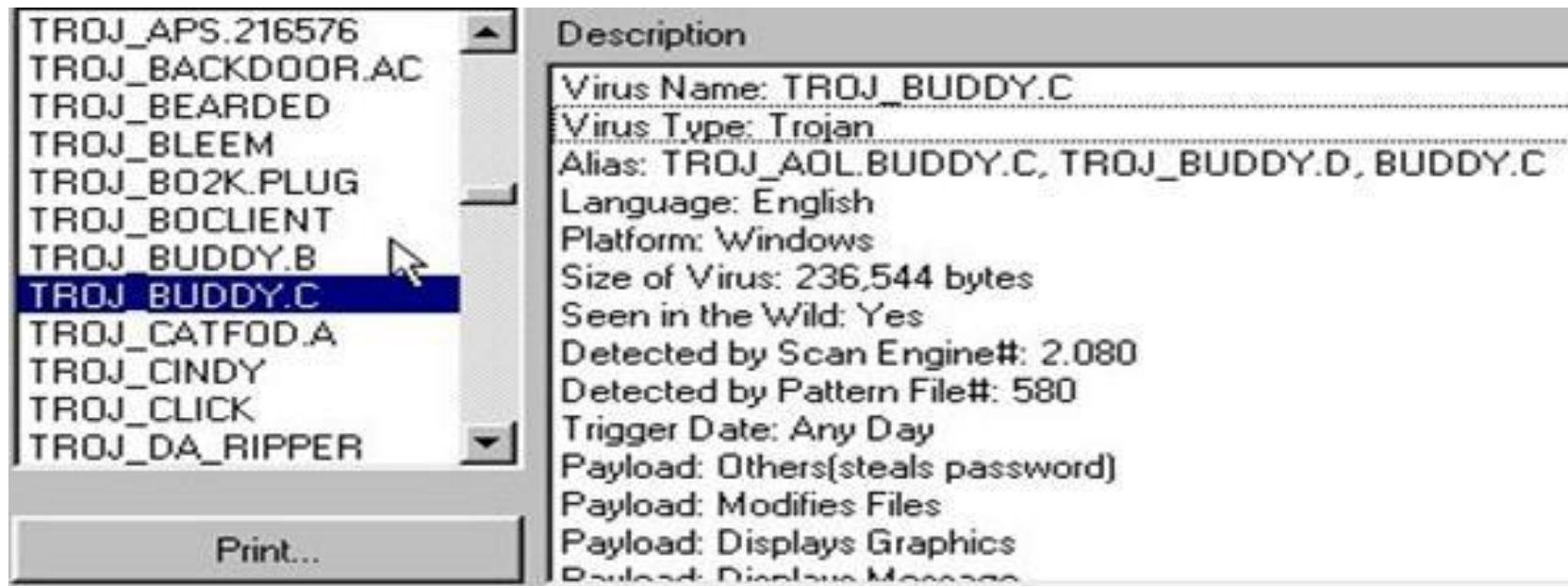
ตัวอย่างเวิร์มที่รู้จักกันอย่างแพร่หลาย เช่น “Nimda”, “W32.Sobig”, “W32.bugbear”, “W32.Blaster” และ “Love Bug” (ซึ่งเป็นไฟล์ที่แนบมากับอีเมลที่กำหนดหัวเรื่องว่า “I LOVE YOU”)



ม้าโทรจัน (Trojan Horse)

เป็นโปรแกรมที่ดูเหมือนจะมีประโยชน์หรือไม่เป็นอันตราย แต่ในตัวโปรแกรมจะแฝงโค้ดสำหรับการใช้ประโยชน์ หรือทำลายระบบที่รัน

ม้าโทรจันจะแตกต่างจากไวรัสและเวิร์ม ตรงที่ม้าโทรจันจะไม่กระจายตัวมันเองไปยังคอมพิวเตอร์เครื่องอื่น ๆ ได้โดยโปรแกรมม้าโทรจันจะแฝงตัวอยู่กับโปรแกรมอื่น ๆ ที่อาจส่งผ่านมาทางอีเมล เช่น Zipped_files.exe และเมื่อมีการเรียกใช้ไฟล์ โปรแกรมจะลบไฟล์ที่อยู่ในฮาร์ดดิสก์

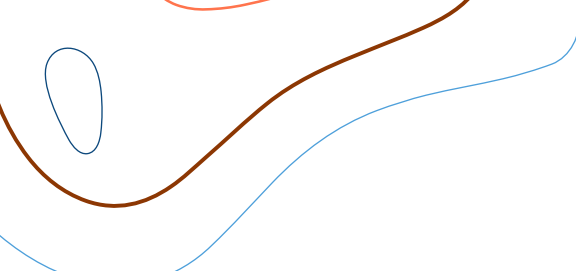


ตัวอย่างไวรัสม้าโทรจัน (Trojan Horse)



ข่าวหลอกลวง (Hoax)

เป็นการส่งข้อความต่อ ๆ กันเหมือนอีเมลลูกโซ่เพื่อให้เกิดความเข้าใจผิด โดยอาศัยเทคนิคทางจิตวิทยาทำให้ข่าวนั้นน่าเชื่อถือ

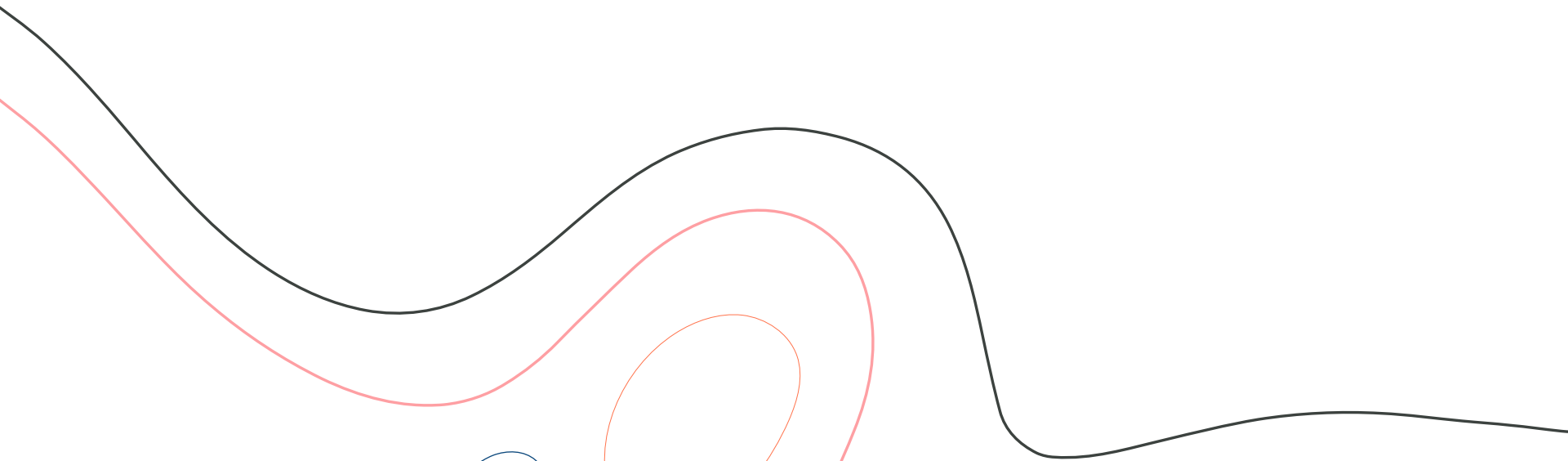


มีข้อสังเกตเพื่อใช้ในการตรวจสอบว่าเครื่องคอมพิวเตอร์ที่กำลังใช้งานอยู่ติดไวรัสหรือไม่

เช่น มีข้อความหรือภาพแปลก ๆ แสดงบนจอภาพ มีเสียงที่ผิดปกติหรือเสียงเพลงเปิดขึ้นเป็นบางเวลา หน่วยความจำคอมพิวเตอร์ลดน้อยลงกว่าที่ควรจะเป็น เครื่องคอมพิวเตอร์ที่กำลังใช้งานอยู่ทำงานช้าผิดปกติ โปรแกรมหรือไฟล์หายไปโดยที่ผู้ใช้ไม่ได้ลบทิ้ง มีโปรแกรมแปลกปลอมเข้ามา ขนาดของไฟล์ใหญ่ผิดปกติ การทำงานของไฟล์หรือโปรแกรมผิดปกติไปจากเดิมที่เคยใช้

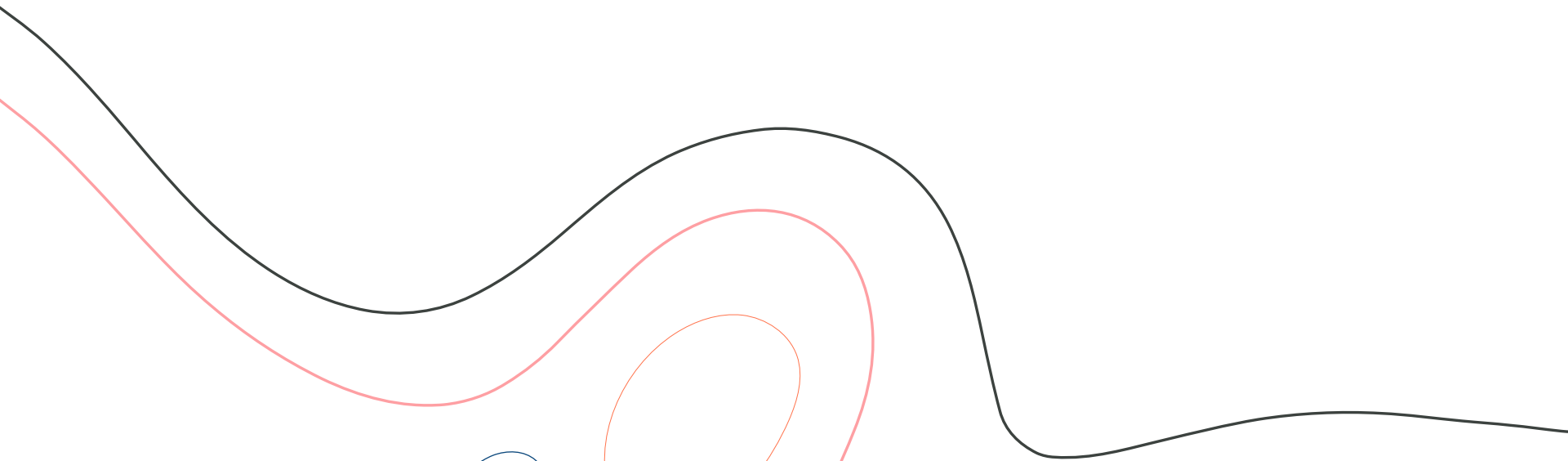
03 การทำให้ระบบปฏิเสธการให้บริการ (Denial of Service)

การทำให้ระบบคอมพิวเตอร์ปฏิเสธการให้บริการ หรือ DoS เป็นการโจมตีเว็บไซต์เพื่อไม่ให้เว็บไซต์นั้นติดต่อสื่อสารกับคอมพิวเตอร์เครื่องอื่น ๆ ได้ การโจมตีอาจมาจากคอมพิวเตอร์เพียงเครื่องเดียว หรือจากคอมพิวเตอร์จำนวนมากที่ถูกควบคุมสั่งการ (Distributed Denial of Service : DDoS)



04 การขโมยคอมพิวเตอร์

การขโมยเครื่องคอมพิวเตอร์และอุปกรณ์ที่เกี่ยวข้องก็เป็นปัญหาอาชญากรรมอย่างหนึ่ง โดยเฉพาะเครื่องคอมพิวเตอร์ที่อยู่ตามสำนักงานของหน่วยงานภาครัฐ หรือเอกชน ที่เก็บข้อมูลสำคัญ ๆ เอาไว้ อาจจะมีผู้ประสงค์ร้ายต้องการนำข้อมูลที่เก็บอยู่ในเครื่องนั้นมาใช้งาน หรือทำลายทิ้งเพื่อปกปิดความลับบางอย่าง



คอมพิวเตอร์ในฐานะ “เป็นเป้าหมายของอาชญากรรม”

01

การเข้าถึงและการใช้คอมพิวเตอร์
โดยไม่ได้รับอนุญาต

02

การก่อกวนหรือการทำลายข้อมูล

03

การทำให้ระบบปฏิเสธการให้บริการ
(Denial of Service)

04

การขโมยคอมพิวเตอร์

03

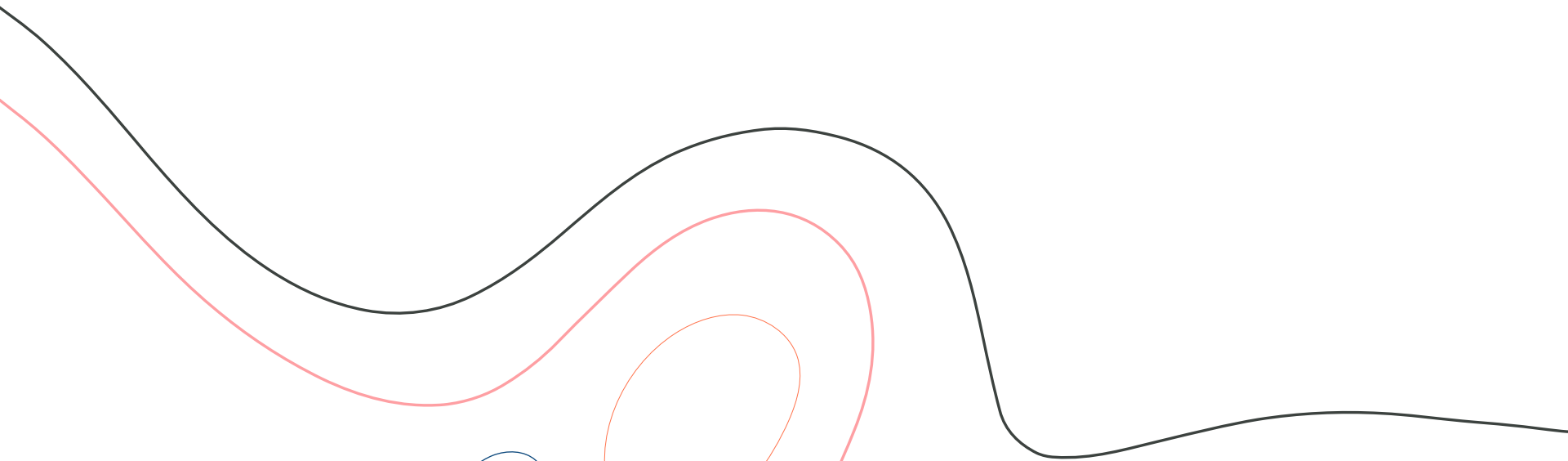
วิธีการป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์

01

การใช้ User name หรือ User ID และรหัสผ่าน (Password)

บางระบบจะกำหนดชื่อผู้ใช้และรหัสผ่านมาให้เพื่อความสะดวก ในขณะที่บางระบบจะให้ผู้ใช้กำหนดเอง หากระบบใดมีการกำหนดรหัสผ่านมาให้ ผู้ใช้ควรเปลี่ยนแปลงรหัสผ่านนั้นใหม่ด้วยตนเองในภายหลัง

และควรหลีกเลี่ยงการกำหนดรหัสที่เป็นวันเดือนปีเกิด เบอร์โทรศัพท์ หรือรหัสอื่น ๆ ที่แฮกเกอร์สามารถเดาได้ง่าย ควรตั้งรหัสผ่านที่มีทั้งตัวอักษรและตัวเลข ๆ



02 การใช้วัตถุใด ๆ เพื่อการเข้าสู่ระบบ

ได้แก่ บัตร หรือกุญแจ ตัวอย่างเช่น การใช้บัตร ATM เพื่อทำธุรกรรมเกี่ยวกับบัญชีธนาคาร ซึ่งโดยปกติจะใช้บัตรควบคู่กับ PIN (Personal Identification Number) ประกอบด้วยตัวเลข 4 หลักและ PIN ก็เป็นรหัสผ่านที่เจ้าของควรให้ความสำคัญ ไม่ควรใช้ตัวเลขที่เกี่ยวกับวันเดือนปีเกิด หรือการจดรหัสลงในบัตร

03 การใช้อุปกรณ์ทางชีวภาพ (Biometric Devices)

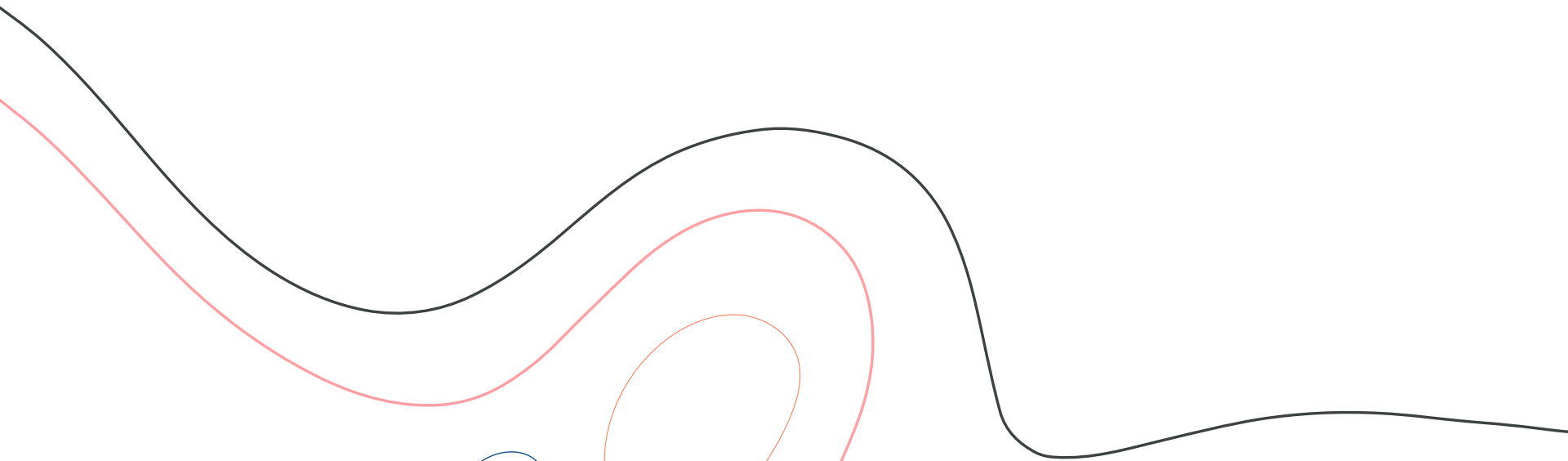
เป็นการใช้อุปกรณ์ตรวจสอบลักษณะส่วนตัวของบุคคลเพื่อการอนุญาตใช้โปรแกรม ระบบ อุปกรณ์ หรือการเข้าใช้ห้องคอมพิวเตอร์ เช่น การตรวจสอบด้วยเสียง ลายนิ้วมือ ฝ่ามือ ลายเซ็น ม่านตา และรูปหน้า เป็นต้น

โดยอุปกรณ์จะทำการแปลงลักษณะส่วนบุคคลให้อยู่ในรูปข้อมูลดิจิทัล แล้วเปรียบเทียบกับข้อมูลที่จัดเก็บในคอมพิวเตอร์ ถ้าข้อมูลไม่ตรงกันคอมพิวเตอร์ก็จะปฏิเสธการเข้าสู่ระบบ

04 ระบบเรียกกลับ (Callback System)

หรือ OTP (On Time Password) เป็นระบบที่ผู้ใช้ระบุชื่อและรหัสผ่าน เพื่อขอเข้าใช้ระบบปลายทาง หากข้อมูลถูกต้อง คอมพิวเตอร์ก็จะเรียกกลับให้เข้าใช้งานเอง

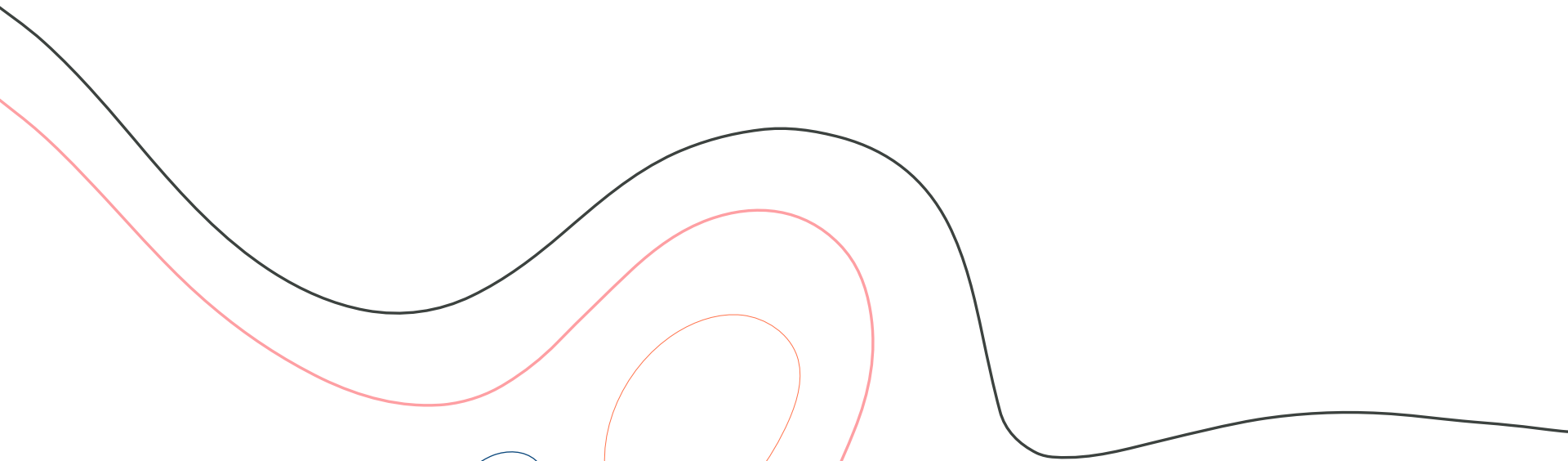
ระบบในลักษณะนี้เป็นการเพิ่มความปลอดภัยให้คอมพิวเตอร์อีกระดับหนึ่ง คือคอมพิวเตอร์จะตรวจสอบหมายเลขโทรศัพท์ของผู้ใช้เมื่อเรียกกลับ



05 เครื่องคอมพิวเตอร์ที่ใช้งานต้องติดตั้งโปรแกรมสแกนไวรัส สแกนสิ่งแปลกปลอมที่จะเข้ามาในเครื่อง และ
อัปเดตฐานข้อมูลไวรัสอย่างสม่ำเสมอ

06 อย่าดาวน์โหลดโปรแกรม ในเว็บไซต์ที่มีความเสี่ยง

07 สำรองข้อมูลต่าง ๆ ที่มีในเครื่องไว้ กรณีฉุกเฉินจะสามารถนำกลับมาใช้ใหม่ได้ หรือใส่รหัสผ่านในการเปิดไฟล์
รหัสผ่านสำหรับแก้ไขเปลี่ยนแปลงไฟล์ที่สำคัญ ๆ





ระบบที่ผู้ใช้ระบุชื่อและรหัสผ่าน เพื่อขอเข้าใช้ระบบปลายทาง หากข้อมูลถูกต้อง คอมพิวเตอร์ก็จะเรียกกลับให้เข้าใช้งานเอง เป็นวิธีการป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์ แบบใด

การใช้วัตถุใด ๆ เพื่อการเข้าสู่ระบบ

การใช้อุปกรณ์ทางชีวภาพ

ระบบเรียกกลับ (Callback System)

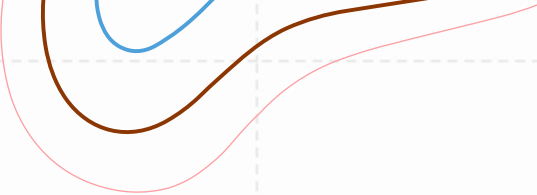


การตรวจสอบด้วยเสียง ลายนิ้วมือ ฝ่ามือ ลายเซ็น ม่านตา และรูปภาพ เป็น
วิธีการป้องกันการเข้าถึงข้อมูลและคอมพิวเตอร์ แบบใด

การใช้วัตถุใด ๆ เพื่อการเข้าสู่ระบบ

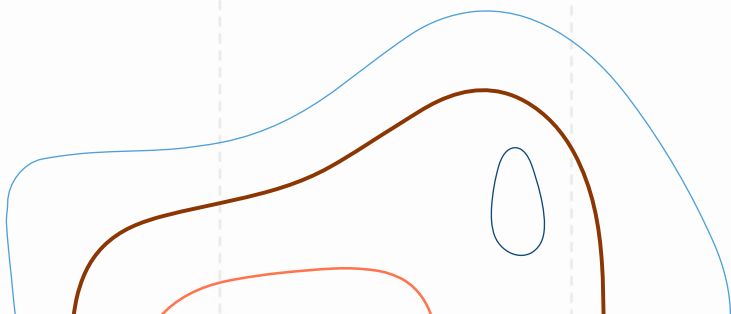
การใช้อุปกรณ์ทางชีวภาพ

ระบบเรียกกลับ (Callback System)



04

ข้อควรระวังในการเข้าไปยังโลกไซเบอร์
หรือใช้งานอินเทอร์เน็ต



01

บัตรเครดิตและการแอบอ้าง

1) ถ้ามีการกรอกข้อมูลส่วนตัวควรใช้เฉพาะเว็บไซต์ที่มีระบบรักษาความปลอดภัย เช่น <https://> หรือ ตรวจสอบชื่อเว็บไซต์หรือ URL ว่าเป็นชื่อเดียวกันกับเว็บที่เคยใช้บริการหรือไม่ทุกครั้ง เพราะมีจฉฉฉฉ อาจจะทำเว็บไซต์ปลอมที่ตั้งชื่อเว็บและมีหน้าตาของเว็บเหมือนหรือคล้ายกับเว็บที่เราเคยใช้มาก ถ้าไม่สังเกตดี ๆ เพื่อหลอกให้ผู้ใช้ กรอกข้อมูลส่วนตัวในการทำธุรกรรม ต่าง ๆ ผ่านเว็บ

2) ให้หมายเลขบัตรเครดิตเฉพาะบริษัทที่ผู้ใช้ไว้วางใจได้เท่านั้น

3) ใช้รหัสผ่านอย่างน้อย 10 ตัวอักขระ (ควรผสมระหว่างตัวอักษรและตัวเลข)

4) ใช้รหัสผ่านที่แตกต่างกันในแต่ละระบบหรือเว็บไซต์



02 การป้องกันข้อมูลส่วนบุคคล

พิจารณาอย่างรอบคอบก่อนการให้ข้อมูลส่วนตัว และให้ข้อมูลในส่วนที่จำเป็น เฉพาะบุคคลนั้น ๆ เท่านั้น

03 การหลีกเลี่ยงสแปมเมลล์

สแปมเมลล์อาจก่อความรำคาญแก่ผู้ใช้อินเทอร์เน็ตได้อย่างมาก เนื่องจากมันจะทวีจำนวนขึ้นเรื่อย ๆ ถ้าผู้ใช้ให้ที่อยู่อีเมลแก่บริษัทที่ทำธุรกิจออนไลน์ ดังนั้นจึงต้องระมัดระวังการลงทะเบียนเพื่อรับข่าวสาร กลับมายังอีเมลของผู้ใช้

04 การป้องกันระบบคอมพิวเตอร์และเครือข่าย

ใช้ไฟร์วอลล์ (Firewall) ที่เป็นฮาร์ดแวร์หรือซอฟต์แวร์เพื่อทำหน้าที่เป็นยามประตูตรวจสอบการเข้าระบบของผู้บุกรุกที่ไม่หวังดี ติดตั้งโปรแกรมสแกนไวรัส สแกนหนอน และมัลแวร์ที่เครื่องคอมพิวเตอร์หรือโทรศัพท์มือถือ

05 อย่ารับหรือเปิดอ่านอีเมล หรือไฟล์ที่แนบมากับอีเมล จากคนที่ไม่รู้จัก

06 ติดตั้งโปรแกรมป้องกันเด็กเข้าถึงเว็บไซต์ที่ไม่พึงประสงค์ เช่น เว็บลามกอนาจาร

07 ติดตามข่าวสารเกี่ยวกับการก่ออาชญากรรมทางคอมพิวเตอร์ จากสื่อต่าง ๆ หรือติดตามข่าวสารเกี่ยวกับการป้องกันการก่ออาชญากรรมและทำลายข้อมูลได้ที่ ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย ที่เว็บไซต์ <https://www.thaicert.or.th/>

แจ้งเตือน พบการส่ง SMS หลอกให้ดาวน์โหลด แอปพลิเคชัน ไทยชนะ แท้จริงเป็นมัลแวร์

เอกสารเผยแพร่ล่าสุด

2020-05-13

รูปแบบการทำงานของแอปพลิเคชันติดตามผู้สัมผัส (contact tracing) ในช่วงการระบาดของ COVID-19 และประเด็นที่ควรพิจารณา

2018-10-03

แนวทางการจัดตั้งศูนย์ปฏิบัติการไซเบอร์เพื่อเฝ้าระวังภัยคุกคาม

2018-04-16

การตั้งค่ากำหนดสิทธิ์การเข้าถึงข้อมูล AWS Bucket

[อ่านเอกสารเผยแพร่ทั้งหมด]

แจ้งเตือนล่าสุด

2020-05-21

ระวังภัย มัลแวร์ WolfRAT โจมตีผู้ใช้ Android ในประเทศไทย สอดแนมการใช้ LINE, Facebook Messenger, และ WhatsApp

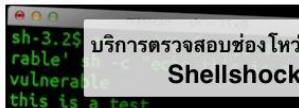
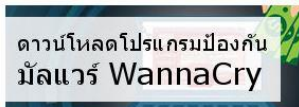
2020-04-09

ระวังภัย พบการโจมตีอุปกรณ์ IoT เพื่อฝังบอทเน็ต dark_nexus ในไทยตกเป็นเหยื่อไม่ต่ำกว่า 172 เครื่อง

2020-03-11

ปฏิบัติการหลายเครือข่าย Necurs botnet มัลแวร์อันตรายที่แพร่กระจายกว่า 9 ล้านเครื่องทั่วโลก

[อ่านแจ้งเตือนทั้งหมด]



เว็บไซต์ <https://www.thaicert.or.th/>

05

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ
คอมพิวเตอร์

สำหรับประเทศไทยมีกฎหมายที่ใช้ลงโทษผู้ที่กระทำความผิดเกี่ยวกับคอมพิวเตอร์และ
เทคโนโลยีสารสนเทศ คือ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550
ประกาศในราชกิจจานุเบกษา เมื่อวันที่ 18 มิถุนายน 2550 เริ่มมีผลบังคับใช้ 18 กรกฎาคม 2550 และ
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

มาตรา ๓ ในพระราชบัญญัตินี้

“ระบบคอมพิวเตอร์” หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ข้อมูลคอมพิวเตอร์” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ข้อมูลจราจรทางคอมพิวเตอร์” หมายความว่า ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับ การติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

“ผู้ให้บริการ” หมายความว่า

(๑) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น

(๒) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น

“ผู้ใช้บริการ” หมายความว่า ผู้ใช้บริการของผู้ให้บริการไม่ว่าต้องเสียค่าใช้บริการหรือไม่ก็ตาม

หมวด ๑ ความผิดเกี่ยวกับคอมพิวเตอร์

มาตรา ๕ ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินหกเดือน หรือปรับไม่เกินหนึ่งหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๖ ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านามาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๗ ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษจำคุกไม่เกินสองปีหรือปรับไม่เกินสี่หมื่นบาทหรือทั้งจำทั้งปรับ

มาตรา ๘ ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักจับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา ๙ ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๐ ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

มาตรา ๑๑ ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ต้องระวางโทษปรับไม่เกินหนึ่งแสนบาท

ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิด ความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับ สามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย ต้องระวางโทษปรับไม่เกิน สองแสนบาท

ให้รัฐมนตรีออกประกาศกำหนดลักษณะและวิธีการส่ง รวมทั้งลักษณะและปริมาณของ ข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ ซึ่งไม่เป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ และลักษณะอันเป็นการบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย

มาตรา ๑๒ ถ้าการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ หรือมาตรา ๑๑ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษา ความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่ สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึง สองแสนบาท

ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นการกระทำต่อข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาท ถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่น ถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๑๒/๑ ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ เป็นเหตุให้เกิดอันตราย แก่บุคคลอื่น หรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท ถ้าการกระทำความผิดตามมาตรา ๙ หรือมาตรา ๑๐ โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่น ถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท

มาตรา ๑๓ ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ ต้องระวางโทษจำคุกไม่เกินหนึ่งปี หรือปรับไม่เกินสองหมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม ต้องระวางโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสี่หมื่นบาท หรือทั้งจำทั้งปรับ

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๘ มาตรา ๙ มาตรา ๑๐ หรือมาตรา ๑๑ หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งดังกล่าวจะต้องรับผิดทางอาญา ตามความผิดที่มีกำหนดโทษสูงขึ้นด้วย ก็เฉพาะเมื่อตนได้รู้หรืออาจเล็งเห็นได้ว่าจะเกิดผลเช่นที่เกิดขึ้นนั้น

ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา ๑๒ วรรคหนึ่งหรือวรรคสาม หากผู้นำไปใช้ได้กระทำความผิดตามมาตรา ๑๒ วรรคหนึ่ง หรือวรรคสาม หรือต้องรับผิดตามมาตรา ๑๒ วรรคสองหรือวรรคสี่ หรือมาตรา ๑๒/๑ ผู้จำหน่าย หรือเผยแพร่ชุดคำสั่งดังกล่าวต้องรับผิดทางอาญาตามความผิดที่มีกำหนดโทษสูงชันนั้นด้วย

ในกรณีที่ผู้จำหน่ายหรือเผยแพร่ชุดคำสั่งผู้ใดต้องรับผิดตามวรรคหนึ่งหรือวรรคสอง และตามวรรคสาม หรือวรรคสี่ด้วย ให้ผู้นั้นต้องรับโทษที่มีอัตราโทษสูงที่สุดแต่กระหนเดียว

มาตรา ๑๔ ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้ ต้องระวางโทษจำคุกไม่เกินห้าปี หรือปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ

(๑) โดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือน หรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหาย แก่ประชาชน อันมิใช่การกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา

(๒) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิด ความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคง ในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิด ความตื่นตระหนกแก่ประชาชน

(๓) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคง แห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(๔) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูล คอมพิวเตอร์นั้น ประชาชนทั่วไปอาจเข้าถึงได้

(๕) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (๑) (๒) (๓) หรือ (๔)

ถ้าการกระทำความผิดตามวรรคหนึ่ง (๑) มิได้กระทำต่อประชาชน แต่เป็นการกระทำต่อบุคคลใด บุคคล หนึ่ง ผู้กระทำ ผู้เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ดังกล่าวต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหก หมื่นบาท หรือทั้งจำทั้งปรับ และให้เป็นความผิดอันยอมความได้

มาตรา ๑๕ ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิด ตามมาตรา ๑๔ ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน ต้องระวางโทษเช่นเดียวกับผู้กระทำความผิด ตามมาตรา ๑๔

ให้รัฐมนตรีออกประกาศกำหนดขั้นตอนการแจ้งเตือน การระงับการทำให้แพร่หลายของ ข้อมูลคอมพิวเตอร์ และการนำข้อมูลคอมพิวเตอร์นั้นออกจากระบบคอมพิวเตอร์

ถ้าผู้ให้บริการพิสูจน์ได้ว่าตนได้ปฏิบัติตามประกาศของรัฐมนตรีที่ออกตามวรรคสอง ผู้นั้นไม่ต้อง รับโทษ

มาตรา ๑๖ ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ ที่ปรากฏเป็น ภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลง ด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย ต้องระวางโทษ จำคุกไม่เกินสามปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำได้ระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง

ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็น การติชม ด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้

ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย

สั่ง

มาตรา ๑๖/๑ ในคดีความผิดตามมาตรา ๑๔ หรือมาตรา ๑๖ ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจ

(๑) ให้ทำลายข้อมูลตามมาตราดังกล่าว

(๒) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใด ตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณา หรือเผยแพร่

(๓) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำ ความผิดนั้น

มาตรา ๑๖/๒ ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลาย ตาม มาตรา ๑๖/๑ ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ ในมาตรา ๑๔ หรือ มาตรา ๑๖ แล้วแต่กรณี

มาตรา ๑๗ ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ

(๑) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(๒) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร

มาตรา ๑๗/๑ ความผิดตามมาตรา ๕ มาตรา ๖ มาตรา ๗ มาตรา ๑๑ มาตรา ๑๓ วรรคหนึ่ง มาตรา ๑๖/๒ มาตรา ๒๓ มาตรา ๒๔ และมาตรา ๒๗ ให้คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้ง มีอำนาจเปรียบเทียบได้ คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็น พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา

เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับ ตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกัน ตามประมวลกฎหมายวิธีพิจารณาความอาญา

ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่ นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว

หมวด ๒ พนักงานเจ้าหน้าที่

มาตรา ๒๖ ผู้ให้บริการต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้ไม่น้อยกว่าเก้าสิบวัน นับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ แต่ในกรณีจำเป็น พนักงานเจ้าหน้าที่จะสั่งให้ผู้ให้บริการผู้ใด เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ไว้เกินเก้าสิบวันแต่ไม่เกินสองปีเป็นกรณีพิเศษเฉพาะราย และเฉพาะคราวก็ได้

ผู้ให้บริการจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ให้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การให้บริการสิ้นสุดลง

ความในวรรคหนึ่งจะใช้กับผู้ให้บริการประเภทใด อย่างไร และเมื่อใด ให้เป็นไปตามที่รัฐมนตรีประกาศในราชกิจจานุเบกษา

ผู้ให้บริการผู้ใดไม่ปฏิบัติตามมาตรานี้ ต้องระวางโทษปรับไม่เกินห้าแสนบาท

ตัวอย่าง การกระทำที่เข้าข่ายมีความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และฉบับที่ ๒ พ.ศ. ๒๕๖๐ เช่น

1) ความผิดฐานเป็นแฮกเกอร์ หรือแอบเข้าไปในเครื่องของผู้อื่น นักเจาะระบบ

บุกรุกเข้าไปในระบบคอมพิวเตอร์ของผู้อื่นที่มีการป้องกันโดยไม่ได้รับอนุญาต จะมีความผิดตาม มาตรา 5 โทษจำคุกไม่เกิน 6 เดือน หรือปรับไม่เกิน 10,000 บาท หรือทั้งจำทั้งปรับ

ถ้ารู้วิธีการป้องกันในการเข้าถึงข้อมูลของผู้อื่นแล้วนำไปเผยแพร่ ทำให้ผู้อื่นเสียหาย มีความผิดตาม มาตรา 6 โทษจำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 20,000 บาท หรือทั้งจำทั้งปรับ

ขโมยหรือแอบใช้ Username และ Password ในการเข้าถึงข้อมูลของผู้อื่น มีความผิดตามมาตรา 7 โทษจำคุกไม่เกิน 2 ปี หรือปรับไม่เกิน 40,000 บาท หรือทั้งจำทั้งปรับ

2) ความผิดเพราะมือบอน ชอบลอบของสร้างหรือปล่อยไวรัส หรือแฮกเกอร์ที่เข้าไปจงใจ แก้ไขทำลายข้อมูลของผู้อื่น จะมีความผิดตามมาตรา 9 โทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ มาตรา 10 โทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

3) ความผิดเพราะอิจฉา ก่อกวนหรือกลั่นแกล้งผู้อื่น ส่งอีเมลขยะไปรบกวนผู้อื่น จะมีความผิดตามมาตรา 11 โทษปรับไม่เกิน 100,000 บาท

4) ความผิดเพราะชอบโพสต์กระทู้ฟอรัมเวิร์ดอีเมล ส่งต่อข้อความ เนื้อหา รูปภาพที่ไม่เหมาะสม หรือแอบอ้าง ใส่ร้ายป้ายสีผู้อื่น เช่น

- 1) ปลอมแปลงไฟล์ เพื่อแฝงตัวเข้าไปทำลายระบบคอมพิวเตอร์ผู้อื่น
- 2) การหลอกลวง ฉ้อโกงผู้อื่น ผ่านเว็บไซต์
- 3) ชอบโพสต์แสดงความคิดเห็น ข้อมูลปลอม โปสต์ข้อความอันเป็นเท็จใส่ร้ายป้ายสีผู้อื่น

แบบไม่มีหลักฐาน หรือหมิ่นประมาทผู้อื่น

- 4) ส่งต่ออีเมล ส่งต่อรูปภาพ ข้อความ คลิปวิดีโอทั้งหลายที่ไม่เหมาะสมกระทบต่อความมั่นคง

ของประเทศ

จะมีความผิดตามมาตรา 14 ต้องโทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

5) จัดทำหรือเผยแพร่เว็บไซต์ลามกอนาจาร โปสต์หรือส่งต่อภาพหรือวิดีโอที่ลามกอนาจาร

จะมีความผิดตามมาตรา 14 โทษจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

6) ความผิดของผู้ดูแลเว็บไซต์ หรือเจ้าของเว็บไซต์ที่ปล่อยปะละเลย

ถ้าเป็นเว็บไซต์ที่เปิดให้สมาชิกสามารถโพสต์ ถาม ตอบ แสดงความคิดเห็น ไม่ว่าจะอยู่ในรูปของข้อความ รูปภาพ หรือคลิปวิดีโอ ที่เข้าข่ายความผิดตามมาตรา 14 แล้วเจ้าของเว็บหรือผู้ดูแลเว็บไม่รีบทำการลบข้อมูลดังกล่าว ก็จะมี ความผิดตามมาตรา 15 โทษเช่นเดียวกับผู้โพสต์ คือจำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 100,000 บาท หรือทั้งจำทั้งปรับ

ผู้ให้บริการหรือเจ้าของเว็บ ต้องเก็บข้อมูลของผู้ใช้บริการไว้อย่างน้อย 90 วัน เพื่อให้สามารถหาตัวผู้กระทำความผิด หากเจ้าหน้าที่ขอตรวจสอบแล้วไม่ได้ทำการเก็บข้อมูลการใช้งานดังกล่าว ก็จะมี ความผิดตามมาตรา 26 โทษปรับไม่เกิน 500,000 บาท

7) ความผิดของผู้ที่ชอบโพสต์ภาพผู้อื่น ไม่ว่าภาพนั้นจะเป็นภาพจริงหรือภาพตัดต่อ

ถ้าภาพนั้นทำให้ผู้อื่นเสื่อมเสียชื่อเสียง อับอาย ถูกเกลียดชัง จะมีความผิดตามมาตรา 16

โทษจำคุกไม่เกิน 3 ปี และปรับไม่เกิน 200,000 บาท แต่ถ้าโพสต์ภาพนั้นโดยสุจริต ก็ถือว่าไม่มีความผิด ความผิดตามมาตรา 16 นี้ สามารถยอมความกันได้