บทที่ 8

การรู้เท่าทันสื่อดิจิทัลและความปลอดภัยยุคดิจิทัล

Digital Media Literacy and Digital Safety

ดร.กฤษณพงศ์ เลิศบำรุงชัย

สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มทร.ธัญบุรี

ความหมายและนิยามของสื่อ

Definition of Media

สื่อ (Media) หมายถึง สื่อหรือการติดต่อให้ถึงกันผ่านช่องทางใดช่องทางหนึ่ง โดยสื่อจะอยู่ในรูปแบบต่าง ๆ เช่น สื่อสิ่งพิมพ์ สื่อดิจิทัล และสื่อธรรมชาติ

ประเภทของสื่อ

Type of Media

สื่อดั้งเดิม

Traditional Media

สื่อสิ่งพิมพ์ สื่อวิทยุ สื่อโทรทัศน์ สื่อภาพยนตร์ และสื่อธรรมชาติ

สื่อใหม่

New Media

สื่อดิจิทัล สื่อปฏิสัมพันธ์ สื่อสังคมออนไลน์ อีเมล์ การสนทนาผ่านเว็บบอร์ด การพูดคุยผ่านโปรแกรมแชท

บทบาทของสื่อในยุคดิจิทัล

Role of Media in The Digital Age

สื่อใหม่มีบทบาทอย่างมากในยุคดิจิทัล เนื่องจากสามารถเสริมสร้างคุณภาพของความรู้ ความคิดเห็นที่หลากลายและเสรี ประกอบด้วย

การให้ข่าวสาร

Information

การประสานสัมพันธ์

Correlation

การสร้างความต่อเนื่องของสังคม

Continuity

การให้ความเพลิดเพลิน

Entertainment

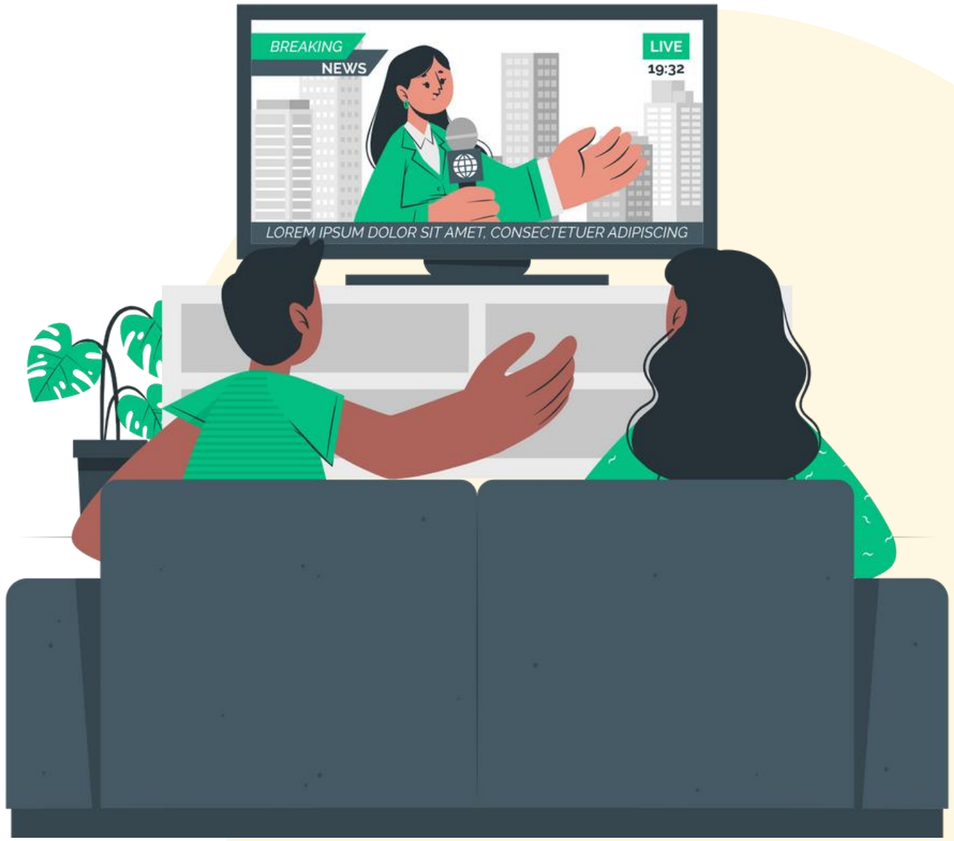
การรณรงค์ทางสังคม การเมือง และเศรษฐกิจ

Mobilization

การให้ข่าวสาร

Information

การให้ข่าวสารเกี่ยวกับเหตุการณ์และสภาพการณ์ในสังคมและโลก ช่วยส่งเสริมให้เกิดความคิดใหม่ๆ การปรับตัว และควาก้าวหน้า



การประสานสัมพันธ์

Correlation

อธิบายและวิพากษ์วิจารณ์ความหมายของเหตุการณ์และข่าวสารต่างๆ เสริมสร้างกระบวนการเรียนรู้ทางสังคม ประสานเชื่อมโยงกลุ่มคนและกิจกรรมต่างๆ เข้าด้วยกัน

การสร้างความต่อเนื่องของสังคม

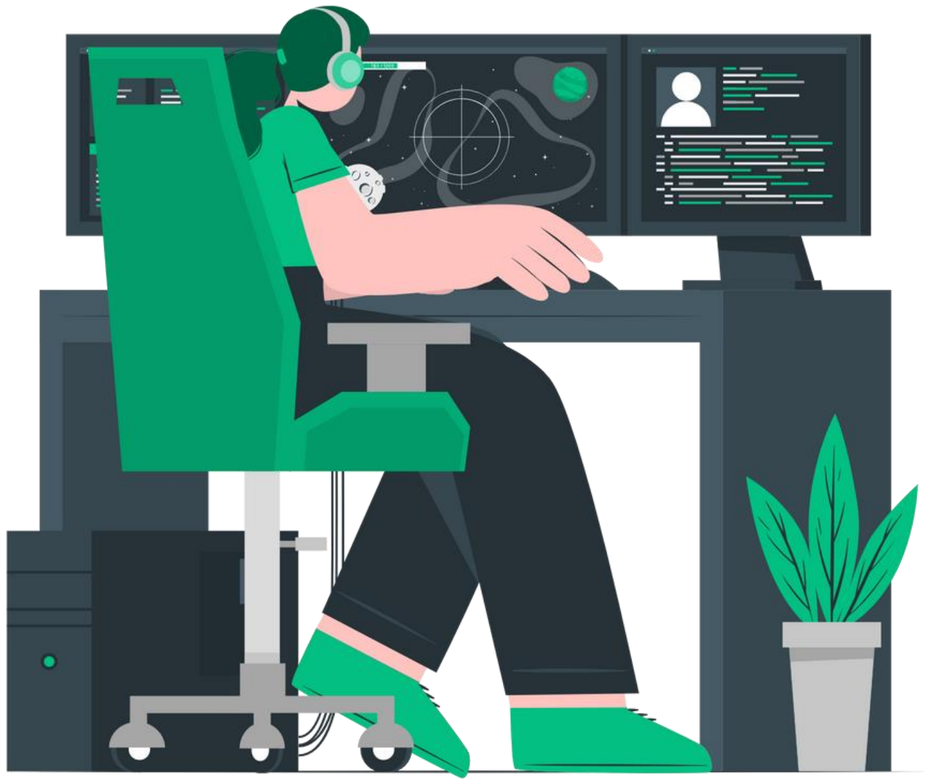
Continuity

ถ่ายทอดวัฒนธรรมหลักและวัฒนธรรมใหม่ๆ เสริมสร้างและดำรงไว้ซึ่งค่านิยมพื้นฐานของสังคม

การให้ความเพลิดเพลิน

Entertainment

ให้ความสนุกสนานเพลิดเพลินและการพักผ่อนหย่อนใจ ลดระดับความเครียด



การรณรงค์ทางสังคม การเมืองและเศรษฐกิจ

Mobilization

รณรงค์ด้านการเมือง สงคราม การพัฒนาทางเศรษฐกิจ และการทำงานเพื่อวัตถุประสงค์ของส่วนรวม

ผู้เผยแพร่สื่อ

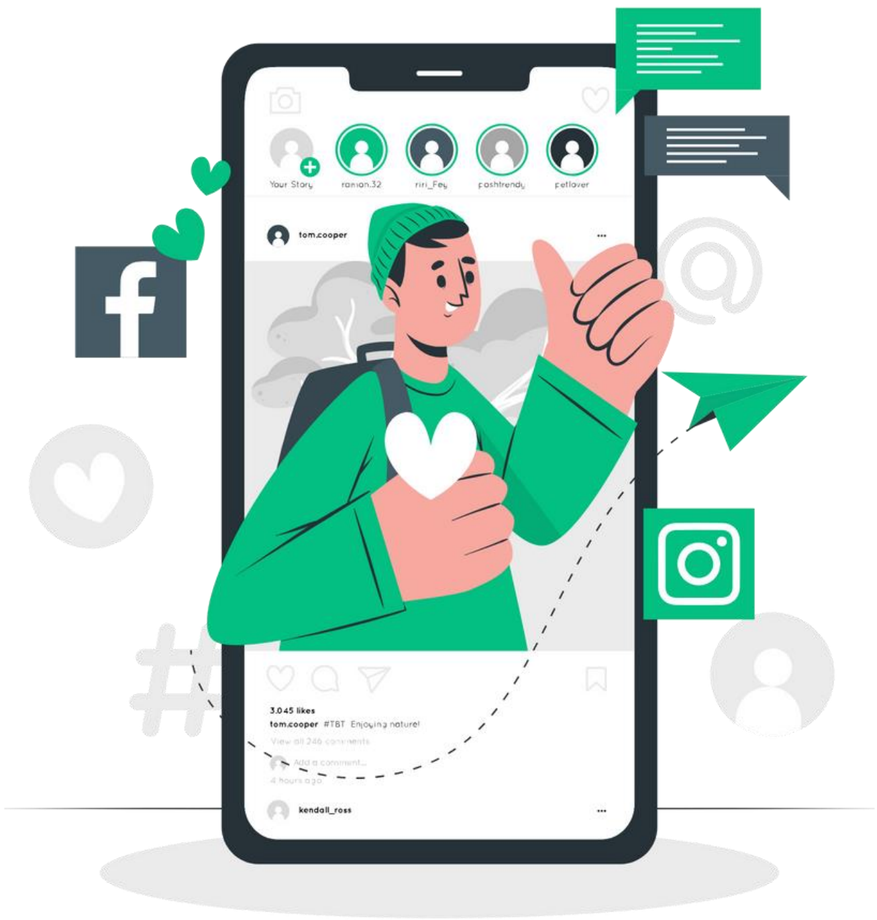
Media Publisher

เผยแพร่สื่อในยุคปัจจุบัน ไม่ได้ถูกจำกัดอยู่แค่นักสื่อสารมวลชนเท่านั้น แต่จะเป็นใครก็ได้ ดังนั้นสื่อที่เผยแพร่ออกมาจะต้องให้ความสำคัญกับเนื้อหาให้ความรู้ ถูกต้อง และเป็นความจริง

การรู้เท่าทันสื่อและสารสนเทศ

Media and Information Literacy: MIL

หมายถึง ความสามารถในการเข้าถึง เข้าใจ กระเมิน ใช้ และสร้างสื่อได้ในหลายรูปแบบ บนความตระหนักของการเข้าถึง ประเมิน และใช้ข้อมูลจากหลายๆ แหล่ง



องค์ประกอบของการรู้เท่าทันสื่อและสารสนเทศ

Components of MIL

การเข้าถึง

Access

เป็นความสามารถในการดึงสื่อและข้อมูลมาใช้

การวิเคราะห์

Analyze

เป็นความสามารถในการวิเคราะห์และสื่อความหมายจากสื่อที่ได้รับรู้

การประเมิน

Evaluate

เป็นความสามารถในการให้คุณค่าจากสื่อที่ได้รับรู้

การสร้างสรรค์เนื้อหา

Create

เป็นความสามารถในการสร้างสรรค์เนื้อหาและนำเสนอได้หลากหลายรูปแบบ

แนวทางการรู้เท่าทันสื่อใหม่

Components of MIL

มิติพื้นที่

Space

มิติเวลา

Time

มิติตัวตน

Self

มิติความเป็นจริง

Reality

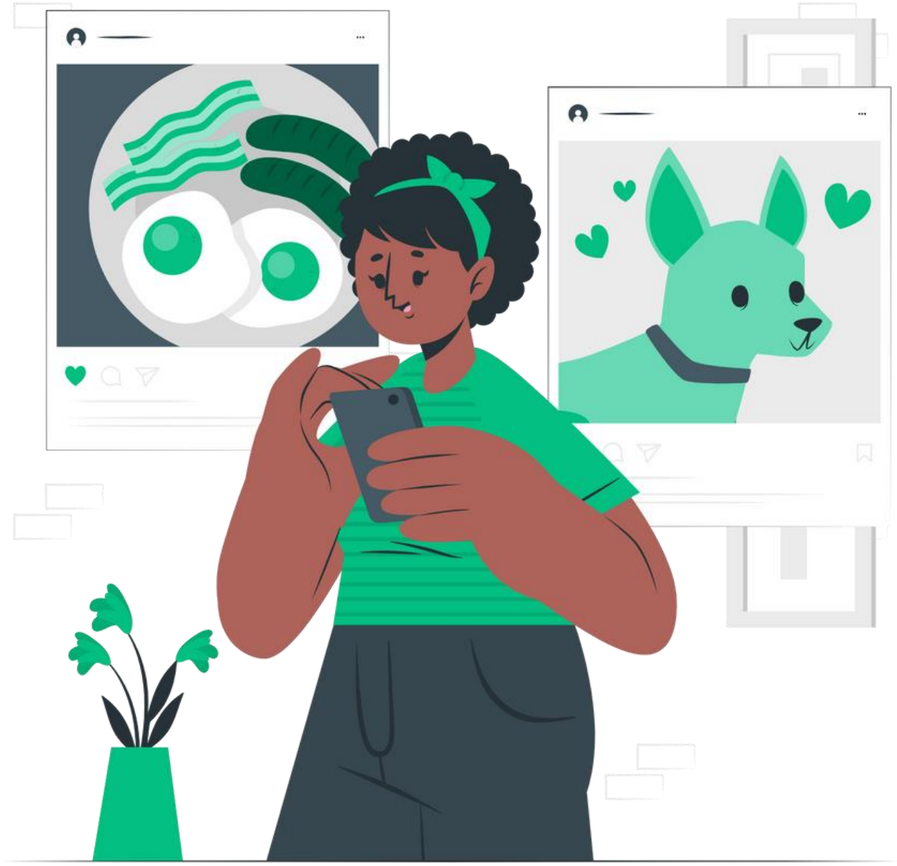
มิติสังคม

Social

มิติพื้นที่

Space

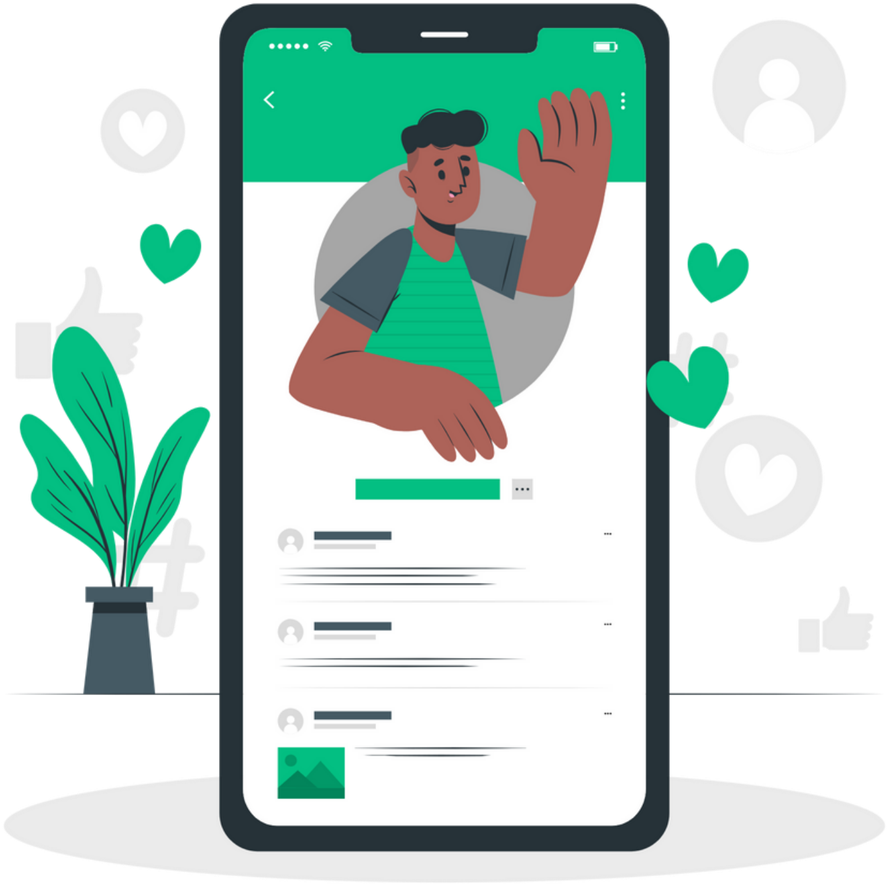
พื้นที่ในยุคดิจิทัลเป็น “พื้นที่ส่วนตัวบนพื้นที่สาธารณะ” ซึ่งเป็นพื้นที่ที่มีคนสร้างขึ้นมาให้เราใช้ เราเป็นเพียงเจ้าของความรู้สึก ดังนั้นสิ่งที่เราโพสต์ออกไปจึงไม่ได้เป็นเพียงพื้นที่ส่วนตัวที่จะโพสต์อะไรก็ได้



มิติเวลา

Time

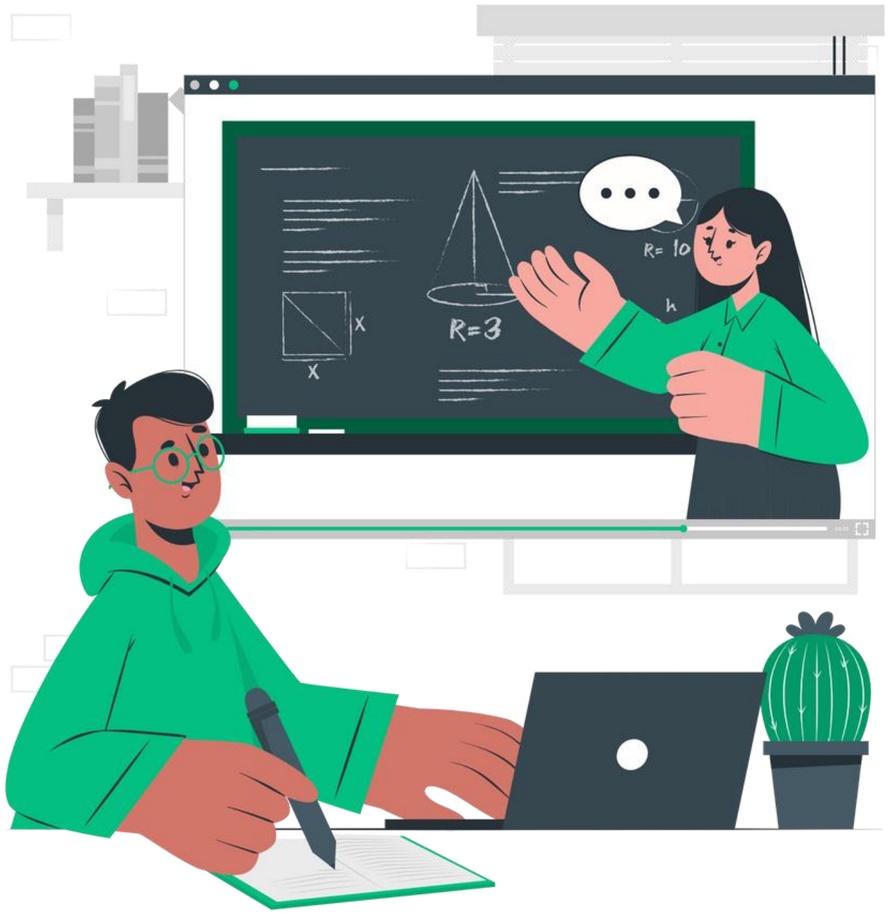
ปัจจุบันมนุษย์ใช้เวลากับสื่อมากขึ้นและหลากหลายในเวลาเดียวกัน ทำกิจกรรมหลายๆ อย่างพร้อมกัน ดังนั้นเราจะต้องรู้เวลาอยู่กับสื่อมากเกินไปหรือไม่ เวลาใดควรใส่ใจกับกิจกรรมอื่น



มิติตัวตน

Self

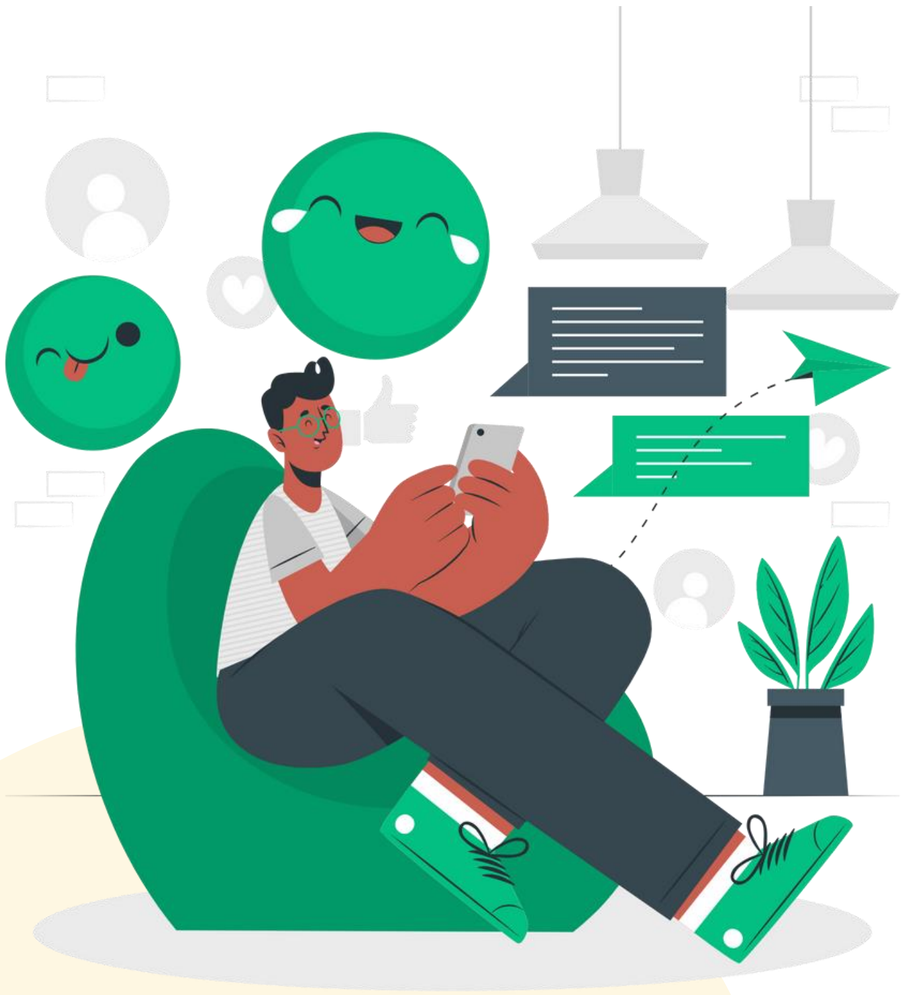
คนในปัจจุบันสามารถสร้างตัวจนจำลองหรืออวตารขึ้นมาเพื่อสร้างอัตลักษณ์บุคคล ซึ่งถ้าหากมันแตกต่างจากตัวตนจริงๆ มาก ย่อมส่งผลด้านลบเชิงจิตวิทยาอัตลักษณ์ตัวตน



มิติความเป็นจริง

Reality

สิ่งที่เรารู้นั้นอาจไม่ใช่ความจริง หรือเป็นข้อเท็จจริงบางส่วน ที่ประกอบกันเพื่อให้เกิดการหลงเชื่อ ดังนั้นผู้ที่รู้เท่าทันสื่อ จะต้องหมั่นศึกษา เรียนรู้ข้อมูลหลายๆ ด้าน



มิติสังคม

Social

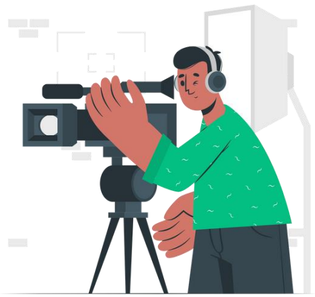
ในโลกดิจิทัลเรามีส่วนสร้างและส่งผลกระทบต่อสังคม การใช้ชีวิต ทัศนคติ ความรู้ พฤติกรรม และจิตวิญญาณ ทุกคนหันมาพูดเรื่องตัวเองมากขึ้นและไม่ใส่ใจจะฟังเรื่องของคนอื่น ทั้งความโกรธ อวดเก่ง ขี้อิจฉา ความรุนแรง อคติ ความเกลียดชัง ต่างถูกโพสต์บนสื่อสังคมออนไลน์ ซึ่งมีพลังทั้งด้านบวกและด้านลบ

การประเมินคุณค่าสื่อและสารสนเทศ

การประเมินองค์กรสื่อ

Media Organizations Evaluation

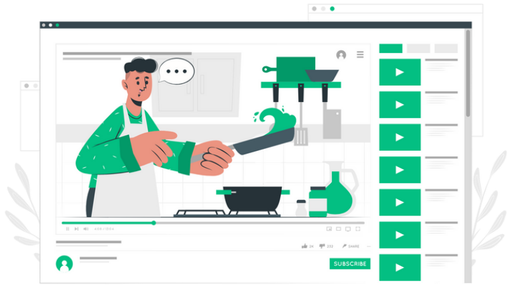
ปัจจุบันองค์กรสื่อมีหลากหลาย มักดำเนินการเพื่อเป้าหมายทางธุรกิจและอยู่ภายใต้การเมือง ผู้รับสื่อจำเป็นต้องศึกษาองค์กรสื่อให้ดีและหลากหลาย เพื่อจะได้นำข้อมูลที่แต่ละองค์กรนำเสนอมาวิเคราะห์



การประเมินผู้ผลิต

Producer Evaluation

ปัจจุบันสื่อไม่จำเป็นต้องมาจากองค์กรเสมอไป ในยุคดิจิทัลใครๆ ก็สามารถเป็นผู้ผลิตได้ ผู้รับสื่อจำเป็นต้องรู้เท่าทันทัศนคติของผู้ผลิตนั้นๆ เพื่อไม่ให้คล้อยตามผู้ผลิตสื่อนั้นๆ ได้ง่าย



การประเมินเนื้อหา

Content Evaluation

ในโลกดิจิทัลมีข้อมูล เนื้อหา มหาศาล เข้ามาหาผู้รับสื่อจำนวนมากในแต่ละวัน ผู้รับสื่อจำเป็นต้องให้ความสำคัญกับสารหรือเนื้อหาที่ผู้ส่งสารส่งมาเกี่ยวกับข้อเท็จจริง ประโยชน์ โทษ และผลกระทบ

ประโยชน์ที่ได้รับจากสื่อ

การเรียนรู้

Learning

การอุปโภคบริโภค

Consumption

ความบันเทิง

Entertainment

การสร้างความสัมพันธ์

Building Relationships

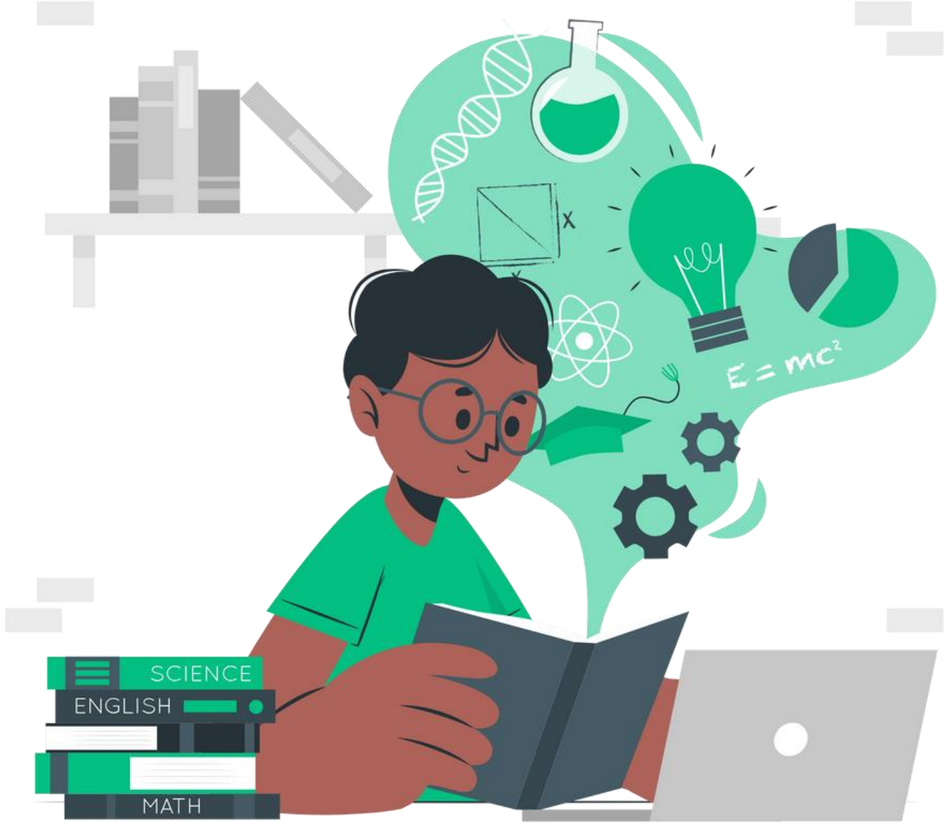
การอาชีพ

Occupation

การเรียนรู้

Learning

สื่อมักให้ความรู้ สร้างความน่าสนใจในการเรียนรู้ ทำให้เกิดการเรียนรู้ได้อย่างมีประสิทธิภาพ



การอุปโภคบริโภค

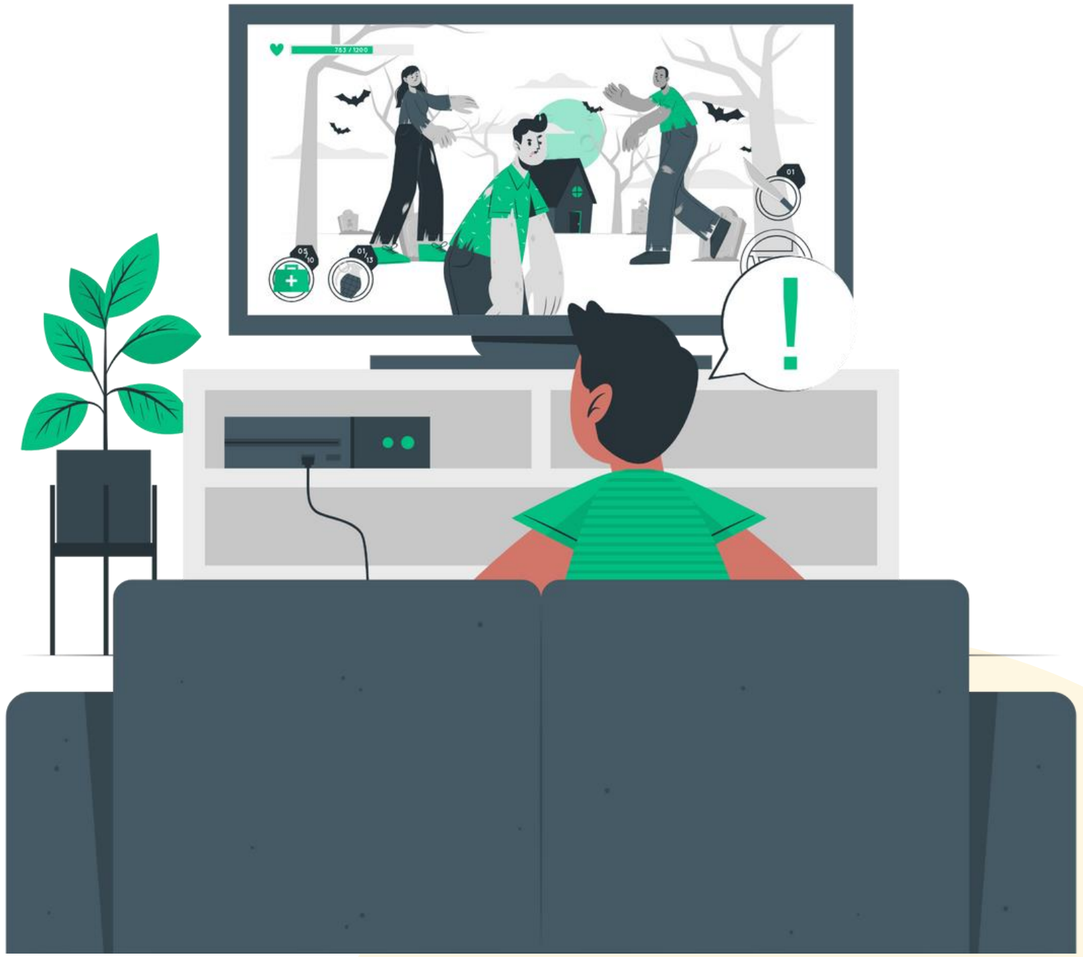
Consumption

สื่อโดยเฉพาะสื่อโฆษณาเข้ามามีบทบาทต่อการดำรงชีวอตเป็นอย่างมาก สร้างความเข้าใจในคุณสมบัติของสินค้าและบริการ สร้างแรงกระตุ้นให้เกิดความอยากใช้ สร้างความภาคภูมิใจในสินค้าและบริการ และสร้างแรงจูงใจในการเลือกซื้อสินค้าและบริการ

ความบันเทิง

Entertainment

สื่อประเภทภาพยนตร์ ดนตรี ซีรีส์ สื่อสังคมออนไลน์ สื่อโทรทัศน์และวิทยุ มักเป็นสื่อที่สร้างความสนุกสนานเพลิดเพลินและผ่อนคลาย ทำให้ลดความเครียดและสร้างความสุข



การสร้างความสัมพันธ์

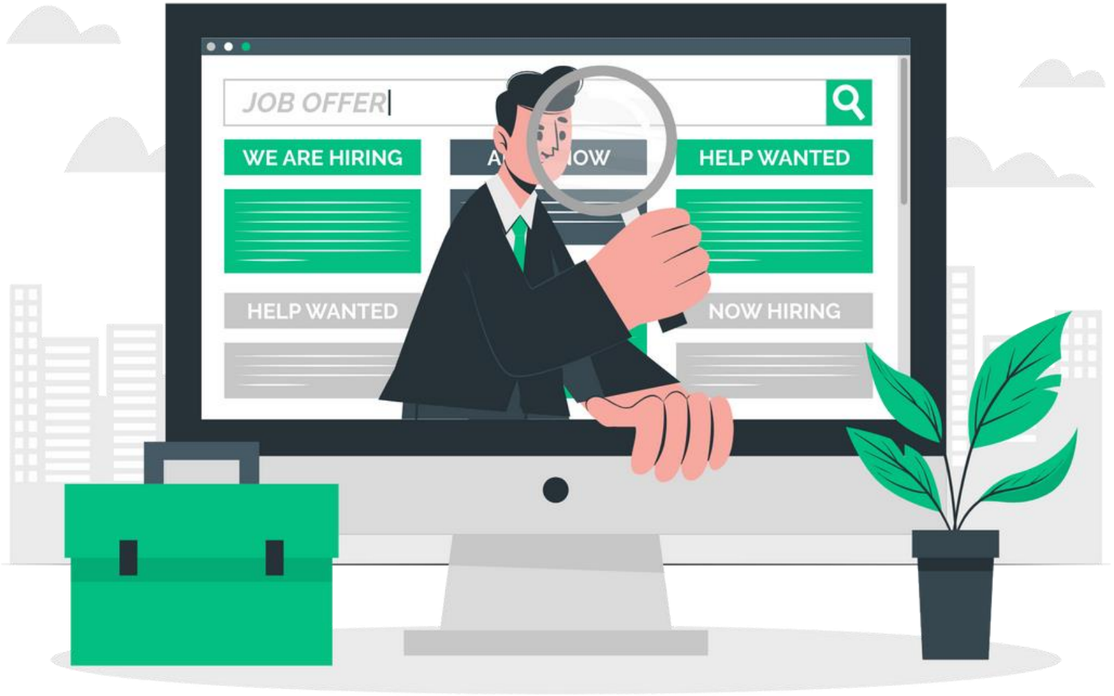
Building Relationships

สื่อสังคมออนไลน์ทำให้ผู้คนต่างๆ สามารถพูดคุย สนทนา แลกเปลี่ยนความรู้ ทำงานร่วมกันได้ตลอดเวลา สร้างความสัมพันธ์ใหม่ๆ คอนเน็คชั่นใหม่ๆ โอกาสใหม่ๆ ได้

การอาชีพ

Occupation

ปัจจุบันมีอาชีพใหม่ๆ เกิดขึ้นมากมาย ที่สร้างรายได้ ทุกอาชีพจำเป็นต้องมีการปรับตัวให้เกิดโอกาสในการหารายได้และเป็นที่รู้จักในวงกว้าง



การรู้เท่าทันข่าวปลอม

Fake News Literacy

ความหมายของข่าวปลอม

Definition of Fake News

ลักษณะของข่าวปลอม

Characteristics of Fake News

ประเภทข่าวปลอม

Types of Fake News

วิธีการตรวจสอบข่าวปลอม

How to Detect Fake News

ความหมายของข่าวปลอม

Definition of Fake News

ข่าวปลอม (Fake News) คือ ข้อมูลเท็จ อาจมีการปลอมบางส่วนหรือทั้งหมด ที่นำเสนอเพื่อสร้างความเสียหายต่อบุคคล หน่วยงาน และสังคม ปัจจุบันข่าวสารต่างๆ ส่งมาทางเทคโนโลยีสารสนเทศ ทำให้ข่าวถูกเผยแพร่และส่งต่อได้ง่ายทั้งแบบตั้งใจและแบบไม่ตั้งใจ

ลักษณะของข่าวปลอม

Characteristics of Fake News

ข่าวปลอม เป็นข่าวที่มีข้อมูลเท็จ ไม่ว่าจะบางส่วนหรือปราศจากข้อเท็จจริงเลย กระตุ้นให้เกิดการแชร์ออกไป เจตนาที่จะบิดเบือนหรือปิดบังความจริงด้วยการใช้อารมณ์มากกว่าเหตุผล และกระตุ้นอคติของผู้อ่าน มีลักษณะดังนี้

Share

Mis-information

เป็นการแชร์ข่าวปลอมโดยไม่ได้ตั้งใจ ผู้ส่งสารไม่มีเจตนาปั่นป่วนหรือทำร้ายใคร แต่แชร์เพราะความไม่รู้

Dis-information

เป็นข่าวปลอมที่ตั้งใจปั่นป่วน ให้ร้าย โจมตีผู้อื่น มีเจตนาที่จะชักนำความคิดของสังคม และปิดบังความจริง

Mal-information

เป็นข่าวปลอมที่สร้างความเกลียดชัง มีข้อเท็จจริงอยู่บ้างแต่เจตนาสร้างขึ้นเพื่อดูถูก เหยียดหยาม สร้างความเกลียดชังให้ผู้ตกเป็นข่าว ข่าวประเภทนี้ส่งผลกระทบร้ายแรงที่สุด

ประเภทข่าวปลอม

Types of Fake News

ข่าวพาดหัว ยั่วให้คลิก

Clickbait

โฆษณาชวนเชื่อ

Propaganda

ข่าวแฝงการโฆษณา

Sponsored Content

ข่าวล้อเลียนและเสียดสี

Satire and Hoax

ข่าวที่ผิดพลาด

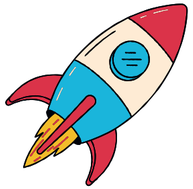
Error

ข่าวเอนเอียงเลือกข้าง

Partisan

ทฤษฎีสมคบคิด

Conspiracy Theory



วิทยาศาสตร์ลวงโลก

Pseudoscience

ข่าวที่ให้ข้อมูลผิดๆ

Misinformation

ข่าวหลอกลวง

Bogus

ข่าวพาดหัว ยั่วให้คลิก

Clickbait

- ใช้คำหรือรูปภาพพาดหัวทำให้ดูชวนสงสัยใคร่รู้
- เนื้อข่าวอาจไม่คำนึงถึงคุณภาพหรือความถูกต้องของข้อมูล
- ทำให้คนหลงกลคลิกเข้าไปเพื่อเรียกยอดวิวในเว็บไซต์

โฆษณาชวนเชื่อ

Propaganda

- มุ่งชักจูงทัศนคติของผู้รับสารต่ออุดมการณ์หรือมุมมองบางอย่าง
- นำเสนอการให้เหตุผลเพียงข้างเดียว
- มักทำซ้ำและกระจายในสื่อหลายชนิดเพื่อหวังผลให้ผู้รับสารเชื่อ

ข่าวแฝงการโฆษณา

Sponsored Content

- รูปแบบโฆษณาที่ใช้รูปแบบเนื้อหาแนบเนียนกับเนื้อหาปกติในเว็บไซต์
- ทำหน้าที่ให้เนื้อหาที่คนต้องการรับรู้โดยไม่ทราบว่าเป็นโฆษณา

ข่าวล้อเลียนและเสียดสี

Satire and Hoax

- ข่าวที่ดัดแปลงข้อมูลเพื่อมุ่งสร้างอารมณ์ขันให้กับผู้อ่าน
- ใช้เนื้อหาที่ตลกขบขันเพื่อแสดงความคิดเห็นเกี่ยวกับเหตุการณ์ข่าว

ข่าวที่ผิดพลาด

Error

- การเขียนข้อความที่ผิด ชื่อบุคคลหรือรูปภาพผิดจากเนื้อข่าว
- ทำให้ผู้รับสารเข้าใจไปในทิศทางอื่น หรือไม่เข้าใจในข่าวนั้น
- บางครั้งสำนักงานข่าวออนไลน์ที่เชื่อถือได้ก็อาจพลาดได้

ข่าวเอนเอียงเลือกข้าง

Partisan

- เป็นข่าวบิดเบือนข่าวสาร
- มักนำเสนอข่าววิพากษ์วิจารณ์ในทางลบต่อฝ่ายที่ตนเองไม่ชอบ
- มักชื่นชมเกินจริงในฝ่ายที่ตนเองสนับสนุน

ทฤษฎีสมคบคิด

Conspiracy Theory

- เกิดจากความคิดของคนที่นำเหตุการณ์มาปะติดปะต่อกัน
- ข้อมูลที่ไม่มีความเชื่อมโยงกัน

วิทยาศาสตร์ลวงโลก

Pseudoscience

- อ้างความเป็นวิทยาศาสตร์แต่ขาดกระบวนการและหลักฐานสนับสนุน
- มาในรูปแบบของบทความทางการแพทย์หรือบทความสุขภาพ
- แฝงโฆษณายารักษาหรืออุปกรณ์เพื่อสุขภาพ
- มีการสร้างภาพผู้เชี่ยวชาญขึ้นมา เพื่อให้ดูน่าเชื่อถือ

ข่าวที่ให้ข้อมูลผิด ๆ

Misinformation

- ข่าวที่ไม่ได้ตรวจสอบให้แน่ชัดเสียก่อน
- อาจมีทั้งจริงและเท็จผสมกัน
- ส่งข่าวต่อโดยไม่รู้และไม่ได้ตระหนัก เช่น ข่าวลือ

ข่าวหลอกลวง

Bogus

- เจตนาในการสร้างขึ้นมาและจงใจให้แพร่กระจาย
- นำเนื้อเรื่อง ภาพ หรือข้อมูลต่างๆ ที่เป็นเท็จมาประกอบกัน
- แอบอ้างเป็นแหล่งข่าวหรือบุคคลที่อยู่ในเหตุการณ์

วิธีการตรวจสอบข่าวปลอม

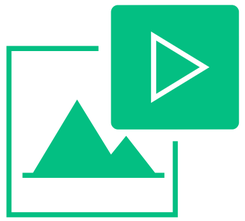
How to Detect Fake News

พิจารณาการ
พาดหัวข่าว

URL เว็บไซต์

ตรวจสอบแหล่งที่มา

ตรวจสอบวันที่



พิจารณารูปภาพ
และวิดีโอ

พิจารณาการพาดหัวข่าว

ข่าวปลอมมักมีข้อความพาดหัวที่สะดุดตา

มีการใช้ตัวหนาและเครื่องหมายอัศเจรีย์ (!)

หัวข้อข่าวดูหวือหวาและไม่น่าเป็นไปได้

URL เว็บไซต์

ปัจจุบัน HTTP ไม่ปลอดภัยมากพอ เว็บไซต์สมัยใหม่จะมีระบบความปลอดภัย (Security) เพื่อความน่าเชื่อถือของเว็บในรูปแบบ HTTPS

ทุกเว็บไซต์จะมีโดเมนเนมนามสกุลต่างๆ เช่น

หากเห็นนามสกุลที่ไม่คุ้นให้สันนิษฐานไว้ว่าอาจเป็นแหล่งข่าวปลอมก็ได้

.com ✓ .org ✓ .co.th ✓ .com.co !

อีกทั้งยังต้องสังเกตจากชื่อ URL ว่าถูกต้องหรือไม่

facebook.com/StarbucksThailand ✓

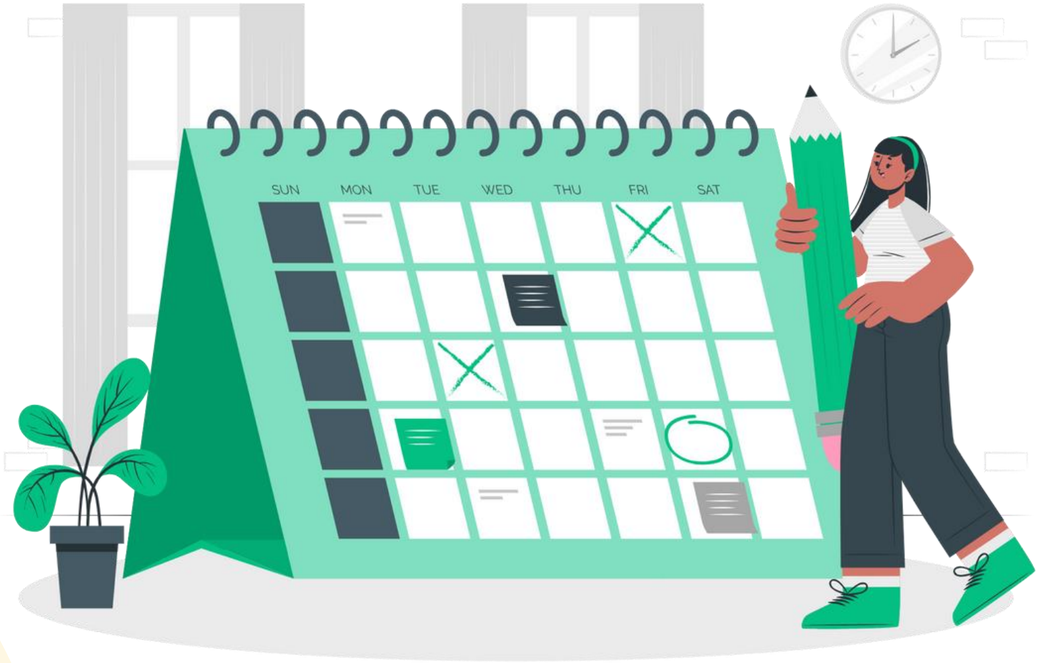
facebook.com/Starbucks_Thailand !

ตรวจสอบแหล่งที่มา

ตรวจสอบให้แน่ใจว่าเรื่องราวนั้นเขียนขึ้นโดยแหล่งข่าวที่น่าเชื่อถือ ถ้าเป็น Facebook ให้ดูข้อมูลเกี่ยวกับ

ตรวจสอบวันที่

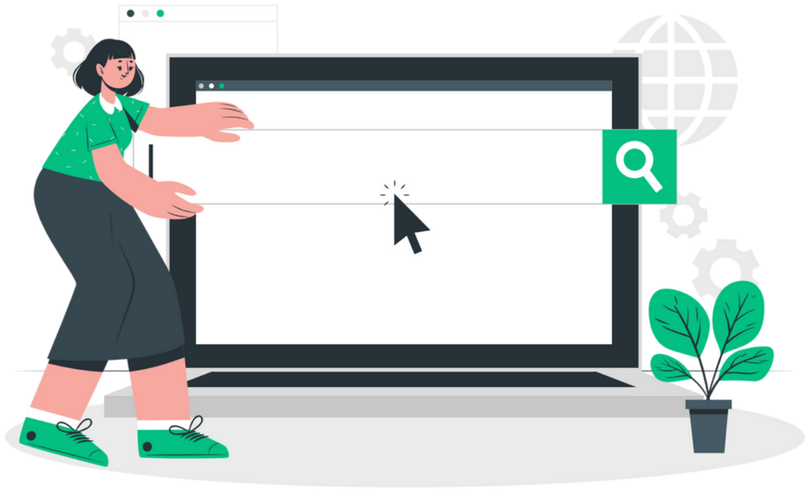
อาจจะเป็นการแชร์ข่าวเก่าที่ผ่านมาแล้ว โดยใช้เครื่องมือ Fact Check อย่าง Google News เป็นบริการที่รวบรวมข่าวทั้งหมดไว้สำหรับค้นหาข่าวโดยเฉพาะ



พิจารณารูปภาพและวิดีโอ

ใช้ Google Image Search ตรวจสอบรูปภาพเบื้องต้นได้

หากต้องการตรวจสอบวิดีโอ ให้แคปเจอร์ฉากสำคัญเป็นภาพนิ่ง แล้วใช้ Google Image Search ตรวจสอบรูปภาพ



รูปแบบไฟล์ดิจิทัล

Digital File Formats

ไฟล์เอกสาร Document Files	ไฟล์รูปภาพ Image Files	ไฟล์บีบอัดข้อมูล Compression files	ไฟล์เสียง Audio Files	ไฟล์วิดีโอ Video files

ไฟล์เอกสาร

.doc / .docx	เป็นไฟล์เอกสารจากโปรแกรม Microsoft Word
.xls / .xlsx	เป็นไฟล์ตารางข้อมูล ตารางคำนวณ จากโปรแกรม Microsoft Excel
.ppt / .pptx	เป็นไฟล์นำเสนอในรูปแบบสไลด์จากโปรแกรม Microsoft PowerPoint
.txt	เป็นไฟล์ Text ธรรมดาจากโปรแกรม Notepad, Wordpad, Microsoft Word หรือ Text Editor ต่างๆ
.pdf	เป็นไฟล์เอกสารขนาดเล็กคุณภาพสูงจาก Adobe ต้องใช้ Adobe Acrobat Reader ในการอ่าน

ไฟล์รูปภาพ

.jpg / .jpeg	เป็นไฟล์ที่ถูกบีบอัดข้อมูลให้มีขนาดเล็ก แต่ยังคงความคมชัด นิยมใช้สร้างเว็บไซต์
.png	เป็นไฟล์ที่ถูกบีบอัดข้อมูลให้มีขนาดเล็ก แต่สูญเสียรายละเอียดของภาพน้อยมาก และสามารถทำภาพโปร่งใสได้ด้วย นิยมใช้บนเว็บไซต์
.gif	เป็นไฟล์ภาพที่ถูกบีบอัดข้อมูลให้มีขนาดเล็กมาก แต่จำกัดสีเพียง 256 สีเท่านั้น สามารถทำภาพโปร่งใสและภาพเคลื่อนไหวได้
.bmp	เป็นไฟล์มาตรฐานของระบบปฏิบัติการ Windows มีขนาดใหญ่
.tiff	เป็นไฟล์ที่ไม่บีบอัดข้อมูล มีความคมชัดสูงมาก มีขนาดไฟล์ที่ใหญ่ เหมาะกับงานสื่อสิ่งพิมพ์
.ai	เป็นไฟล์มาตรฐานของ Adobe Illustrator สามารถบันทึกและเปิดเพื่อแก้ไขได้ตลอดเวลา โดยยังรักษาคุณสมบัติต่างๆ เช่น สี เอฟเฟกต์ เลเยอร์ เอาไว้
.psd	เป็นไฟล์มาตรฐานของ Adobe Photoshop สามารถบันทึกและเปิดเพื่อแก้ไขได้ตลอดเวลา โดยยังรักษาคุณสมบัติต่างๆ เช่น สี เอฟเฟกต์ เลเยอร์ เอาไว้

ไฟล์บีบอัดข้อมูล

.zip เป็นไฟล์ที่ถูกบีบอัดข้อมูลจากระบบปฏิบัติการ

.rar เป็นไฟล์ที่ถูกบีบอัดข้อมูลโดยใช้โปรแกรม WinRAR

ไฟล์วิดีโอ

.avi เป็นไฟล์วิดีโอมาตรฐานของคอมพิวเตอร์ที่มีขนาดใหญ่ เนื่องจากไม่มีการบีบอัดข้อมูล ทำให้ภาพและเสียงมีคุณภาพสูง มีความคมชัด

.mov เป็นไฟล์วิดีโอมาตรฐานของเครื่องแมคอินทอช (Macintosh) แต่สามารถใช้ได้ใน Windows โดยเปิดผ่านโปรแกรม QuickTime Player

.mp4 เป็นไฟล์วิดีโอที่มีขนาดไฟล์เล็ก แต่มีคุณภาพสูง การเข้ารหัสแบบ H.264 จะได้ไฟล์ MP4 ที่ได้รับความนิยมในปัจจุบัน

ไฟล์เสียง

.wav เป็นไฟล์เสียงมาตรฐานที่ใช้กับ Windows มีคุณสมบัติคือครอบคลุมทุกความถี่เสียง ทำให้คุณภาพเสียงดี แต่มีขนาดไฟล์ใหญ่

.mp3 พัฒนามาจาก Motion Picture Experts Group หรือ MPEG โดยมีกระบวนการบีบอีดเสียงให้มีขนาดเล็กลงด้วยวิธีการลด Bit Rate

.ogg เป็นเทคโนโลยีการบีบอัดแบบใหม่ ทำให้มีขนาดไฟล์เล็กกว่า MP3 อยู่ในกลุ่ม Open Source Project และมีความสามารถด้าน Streaming ทำให้ได้รับความนิยมใช้งานบนอินเทอร์เน็ต

.wma พัฒนาโดยบริษัท Microsoft มีลักษณะคล้ายกับไฟล์ MP3 แต่มีขนาดเล็กกว่า เหมาะกับการใช้งานบนอินเทอร์เน็ต

.midi เป็นไฟล์ข้อมูลเสียงดนตรี ที่ถูกสร้างจากชิปสังเคราะห์ (Synthesizer Chip) ไฟล์เสียงมีขนาดเล็ก แต่ต้องใช้โปรแกรม MIDI Player ในการเปิดไฟล์

.m4a เป็นไฟล์มาตรฐานของ Apple ที่ใช้กับโปรแกรม iTune ที่สามารถบีบอัดได้หลายขนาด และสามารถเก็บข้อมูลชื่อเพลงและชื่ออัลบั้มได้

ความปลอดภัยยุคดิจิทัล

Digital Security

ข้อมูลส่วนบุคคลออนไลน์

Online Personal Data

รอยเท้าดิจิทัล

Digital Footprint

การแบ่งปันเนื้อหาในโลกออนไลน์

Sharing Content Online

การกลั่นแกล้งบนโลกออนไลน์

Cyberbullying

ภัยคุกคาม / ภัยอันตราย

Threat

การป้องกันภัยคุกคาม

Threat Protection

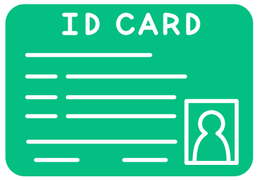
ข้อมูลส่วนบุคคลออนไลน์

Online Personal Data

ข้อมูลส่วนบุคคลที่พบว่ามีการเผยแพร่ในเว็บไซต์ต่าง ๆ ได้แก่

ชื่อ-นามสกุล

Name Surname



เลขประจำตัวประชาชน

Identification Number

ที่อยู่

Address

ภาพถ่ายประจำตัว

Photo

ข้อมูลส่วนบุคคลออนไลน์

Online Personal Data

ข้อมูลส่วนบุคคลที่พบว่ามีการเผยแพร่ในเว็บไซต์ต่าง ๆ ได้แก่

อีเมล E-Mail	หมายเลขโทรศัพท์ Phone Number	สถานที่ทำงาน Place of Work	เลขบัญชีธนาคาร Bank Account Number

รอยเท้าดิจิทัล

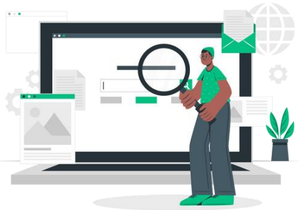
Digital Footprint

ข้อมูลส่วนตัวที่ถูกเผยแพร่บนโลกออนไลน์ จะมีสิ่งที่เรียกว่ารอยเท้าดิจิทัล (Digital Footprint) แบ่งออกเป็น 2 ประเภท ได้แก่

แบบตั้งใจบันทึก

Active Digital Footprint

ประวัติดิจิทัลที่เกิดจากความตั้งใจ เป็นข้อมูลที่เปิดเผยโดยที่เรารู้ตัว เช่น การส่งอีเมล การเขียนบล็อก การโพสต์ข้อความในโซเชียลมีเดีย



แบบไม่ตั้งใจบันทึก

Passive Digital Footprint

ประวัติดิจิทัลที่ไม่ได้เกิดจากความตั้งใจ เป็นข้อมูลที่ไม่มีเจตนาบันทึก เช่น IP Address และประวัติการค้นหา

การแบ่งปันเนื้อหาในโลกออนไลน์

Sharing Content Online

การแบ่งปันเนื้อหาในโลกออนไลน์ มักเกิดจากการที่ผู้ใช้เจตนาเปิดเผยโดยยินยอมหรือรู้ตัว เมื่อข้อมูลถูกอัปโหลดขึ้นไปแล้ว โลกออนไลน์จะบันทึกไว้ในโลกออนไลน์ตลอดไป ดังนั้นสิ่งที่ควรระมัดระวัง ได้แก่

1. ไม่เปิดเผยข้อมูลส่วนบุคคลโดยไม่จำเป็น
2. ไม่เข้าเว็บไซต์ที่ไม่น่าเชื่อถือ เพราะอาจถูกดักจับข้อมูลได้
3. ไม่กรอกข้อมูลจากลิงก์หรือดาวน์โหลดข้อมูลจากแหล่งที่ไม่น่าเชื่อถือ ผู้ที่ไม่หวังดีอาจลักลอบเก็บข้อมูลของเราไปได้
4. ระมัดระวังการโพสต์หรือการให้ข้อมูลกับใครในโลกออนไลน์

อย่างไรก็ตามเราจำเป็นต้องใช้โลกดิจิทัลอย่างหลีกเลี่ยงไม่ได้ เพราะต้องใช้ทำงาน ลงทะเบียน หรืออื่นๆ อีกหลายอย่าง รอยเท้าดิจิทัลก็ยังมีอยู่ดี ดังนั้นเราต้องใช้งานอย่างระมัดระวัง

การกลั่นแกล้งบนโลกออนไลน์

Cyberbullying

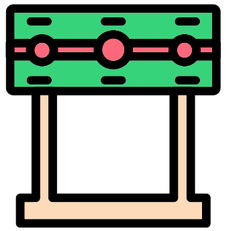
เป็นการกระทำที่ตั้งใจทำให้ผู้อื่นได้รับความทุกข์ความเจ็บปวด ถือเป็นการละเมิดสิทธิมนุษยชน โดยใช้เครื่องมือสื่อสารเป็นหลักและมักเกิดขึ้นในสื่อสังคมออนไลน์ เนื่องจากเข้าถึงง่ายและส่งต่อได้ง่าย

รูปแบบการกลั่นแกล้งบนโลกออนไลน์ที่มักพบบ่อย

Common Forms of Online Bullying

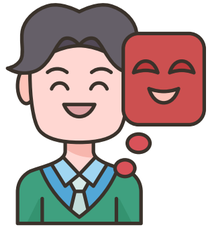
ทำให้อับอาย

Embarrass



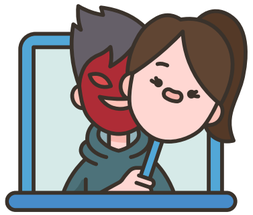
การประจาน

Pillory



การหลอกลวง

Deception



การแอบอ้างตัวตน
ของผู้อื่น

Impersonation

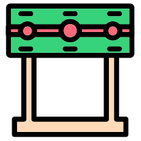
การแบล็กเมล์

Blackmail

ทำให้อับอาย

Embarrass

เป็นการกลั่นแกล้งที่มักใช้ถ้อยคำเชิงลบ เช่น การโพสต์ด่าทอ ล้อเลียน ใส่ร้าย ขู่ทำร้าย พูดจาส่อเสียด เหยียดเพศสภาพและชาติพันธ์ ใช้ถ้อยคำโจมตีให้เกิดความเสียหาย



การประจาน

Pillory

การประจาน เป็นการกลั่นแกล้งโดยการนำคลิปอนาจาร หรือคลิปที่ผู้ถูกกระทำโดนทำร้าย รุมแกล้ง แล้วนำไปโพสต์บนสื่อสังคมออนไลน์ ก่อให้เกิดการแสดงความคิดเห็นที่เสียหายต่อผู้ถูกกระทำ

การหลอกลวง

Deception

เป็นการถูกมิจฉาชีพหลอกลวงให้ผู้คนหลงเชื่อ โดยสวมรอยเป็นบุคคลที่เป็นที่รู้จักในวงกว้างและเป็นที่นับถือ ผู้หลอกโอนเงิน หลอกมีเพศสัมพันธ์ หรือทำอนาจาร

การแอบอ้างตัวตนของผู้อื่น

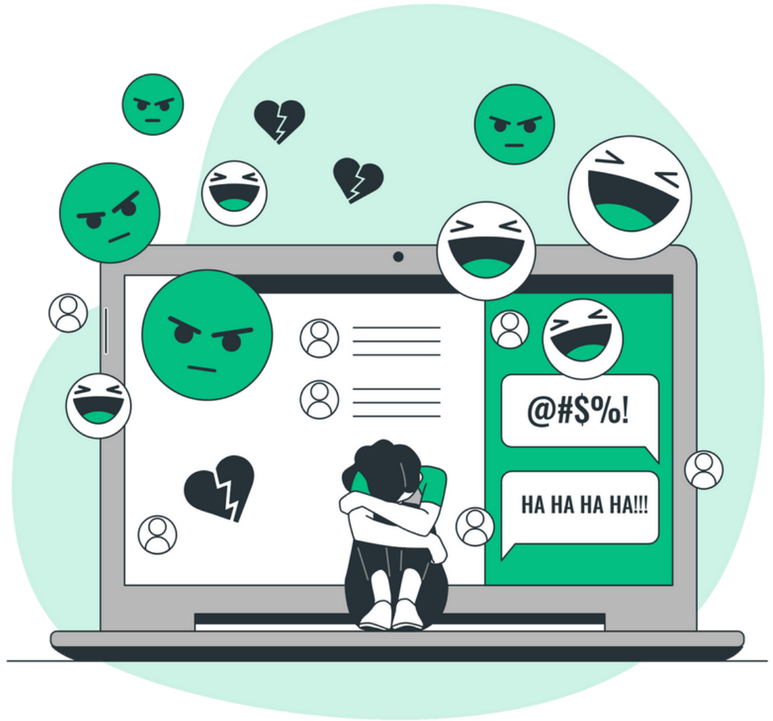
Impersonation

เป็นการกลั่นแกล้งโดยการนำข้อมูลของคนอื่นมาใช้เสมือนเป็นของตัวเอง เช่น การนำโปรไฟล์ของคนอื่นมาแอบใช้สื่อสารกับผู้อื่น การสวมรอยใช้บัญชีผู้ใช้ของคนอื่นโพสต์ถ้อยคำหยาบคาย ให้ร้ายบุคคลอื่น โพสต์รูปนาจาร คลิปวิดีโอลามก

การแบล็กเมล์

Blackmail

เป็นการนำความลับของผู้อื่นาเปิดเผยบนสื่อสังคมออนไลน์ ทำให้มีการแชร์ต่อออกไปอย่างกว้างขวาง เช่น การตัดต่อรูปภาพผู้อื่นไปใช้ในทางไม่เหมาะสม การแอบถ่ายภาพหลุดของผู้อื่นและแชร์ต่อกันโลกออนไลน์



ผลกระทบของการกลั่นแกล้งบนโลกออนไลน์

Impact of Online Bullying

ผลกระทบของการกลั่นแกล้งบนโลกออนไลน์อาจมีตั้งแต่สร้างความรำคาญ ความเดือดเนื้อร้อนใจ บางคนรู้สึกเบื่อชีวิต ไม่อยากไปโรงเรียน ไม่อยากพบเจอใคร บางคนอาจมีความเครียดหนัก ทำให้กินไม่ได้ นอนไม่หลับ และอาจาร้ายแรงถึงขั้นไม่อยากมีชีวิตอยู่ ส่งผลให้รู้สึกอยากฆ่าตัวตาย

การรับมือกับการถูกกลั่นแกล้งบนโลกออนไลน์

Dealing with Cyberbullying

อย่าตอบโต้

Don't Retaliate

เก็บหลักฐานให้พร้อม

Keep Evidence

กดรายงานแล้วบล็อกบัญชีผู้ใช้

Report and Block

ตั้งค่าความเป็นส่วนตัว

Privacy Settings

นัดเจรจากับอีกฝ่ายแบบเจอหน้า

Face to Face

ขอความช่วยเหลือ

Ask for Help

อย่าตอบโต้

Don't Retaliate

การตอบโต้ในรูปแบบเดียวกัน หรือคุกคามอีกฝ่ายเพื่อแก้แค้น ไม่ทำให้อะไรดีขึ้น

เก็บหลักฐานให้พร้อม

Keep Evidence

การแคปเจอร์หน้าจอ และทำการบันทึกเก็บไว้ในคอมพิวเตอร์หรือสมาร์ทโฟน ช่วยเป็นหลักฐานในการดำเนินคดีได้ และควรเก็บข้อมูลไว้บนคลาวด์ เช่น OneDrive, GoogleDrive เผื่ออุปกรณ์ได้รับความเสียหาย ข้อมูลจะยังคงอยู่และนำกลับมาใช้ได้ตลอดเวลา

กดรายงานแล้วบล็อกบัญชีผู้ใช้

Report and Block

กดรายงานแล้วบล็อกบัญชีผู้ใช้ สื่อสังคมออนไลน์จะมีปุ่มรายงานโพสต์หรือรายงานบัญชีผู้ใช้ที่เหมาะสม ให้กด แล้วก็บล็อกบัญชีผู้ใช้นั้น

ตั้งค่าความเป็นส่วนตัว

Privacy Settings

หากกดรายงานหรือบล็อกไปแล้ว ผู้ที่กลั่นแกล้งยังไม่หยุด มีการสมัครบัญชีผู้ใช้ใหม่มากลั่นแกล้งเราอีก ให้ตั้งค่าความเป็นส่วนตัวแบบไม่เปิดสาธารณะ

นัดเจรจากับอีกฝ่ายแบบเจอหน้า

Face to Face

นัดเจรจากับอีกฝ่ายแบบเจอหน้า หากต้องการจบปัญหาความขัดแย้งที่เป็นต้นเหตุของการกลั่นแกล้ง การเจรจากันอย่างสันติเป็นทางออกที่ดี แต่ต้องมีคนกลางอยู่ด้วย และอยู่ในสภาพแวดล้อมที่ควบคุมได้

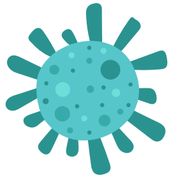
ขอความช่วยเหลือ

Ask for Help

ขอความช่วยเหลือ หากถูกกลั่นแกล้งจนเกินรับมือ เราควรบอกกล่าวปัญหาที่พบเจอกับคนใกล้ตัว หรือคนที่มีอำนาจมากพอที่จะหยุดการกลั่นแกล้งได้ เช่น แจ้งผู้ปกครอง แจ้งครูอาจารย์ หรือแจ้งตำรวจ

ภัยคุกคาม / ภัยอันตราย

Threat



ไวรัส

Virus

หนอน

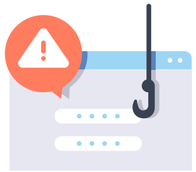
Worms

สปายแวร์

Spyware

แอดแวร์

Adware



ฟิชชิ่ง

Phishing

สแปมเมล์

Spam Mail

แฮกเกอร์

Hacker

แครกเกอร์

Cracker

ไวรัส

Virus

โปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่น ๆ ภายในเครื่องคอมพิวเตอร์ ทำให้ไฟล์เอกสารถูกทำลาย สามารถกระจายไปยังคอมพิวเตอร์เครื่องอื่นได้โดยการใช้สื่อจัดเก็บข้อมูล เช่น ใช้แฟลชไดร์ฟคัดลอกไฟล์ข้อมูล และติดไวรัสเมื่อนำไปใช้กับเครื่องอื่น

หนอน

Worms

โปรแกรมคอมพิวเตอร์ที่ถูกออกแบบมาให้สามารถแพร่กระจายตัวเองจากเครื่องคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง โดยอาศัยระบบเน็ตเวิร์ค (E-mail) ซึ่งการแพร่กระจายสามารถทำได้ด้วยตัวของมันเองอย่างรวดเร็วและทำความเสียหายรุนแรงกว่าไวรัสมาก

สปายแวร์

Spyware

เป็นโปรแกรม เช่น ม้าโทรจัน (Trojan Horse) ที่อาศัยหลอกให้ผู้ใช้ดาวน์โหลดไปติดตั้ง และเปิดโอกาสให้ผู้ไม่ประสงค์ดีเข้ามาเพื่อสังเกตการณ์หรือดักจับข้อมูล หรือควบคุมเครื่องคอมพิวเตอร์ บางโปรแกรมอาจบันทึกว่าผู้ใช้พิมพ์อะไรบ้างเพื่อพยายามค้นหารหัสผ่าน หรือเลขหมายบัตรเครดิต

แอดแวร์

Adware

โปรแกรมที่ดาวน์โหลดสื่อโฆษณาโดยอัตโนมัติขณะที่โปรแกรมกำลังทำงาน สามารถดูได้ผ่านหน้าต่างป๊อปอัปหรือผ่านแถบที่ปรากฏบนหน้าจอคอมพิวเตอร์ หรือแสดงผลบนหน้าจอ ระหว่างกระบวนการติดตั้งโปรแกรมคอมพิวเตอร์

ฟิชชิ่ง

Phishing

การหลอกลวงทางอินเทอร์เน็ตเพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยส่งข้อมูลมาทางออนไลน์ และจำลองตัวเองเหมือนกับหน้าเว็บไซต์ต่างๆ ทำให้ผู้ใช้เข้าใจผิด และกรอกข้อมูลต่างๆ ลงในช่องกรอกข้อมูล

สแปมเมล์

Spam Mail

การส่งข้อความที่ไม่เป็นที่ต้องการให้กับคนจำนวนมากๆ จากแหล่งที่ผู้รับไม่เคยรู้จัก มักอยู่ในรูปของ E-mail ทำให้ผู้รับรำคาญใจ และเสียเวลาในการลบข้อความ ทำให้ประสิทธิภาพการรับส่งข้อมูลบนอินเทอร์เน็ตลดลง

แฮกเกอร์

Hacker

ผู้ที่แอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงานหรือองค์กรอื่นโดยมิได้รับอนุญาต ไม่มีเจตนาที่จะสร้างความเสียหาย หรือสร้างความเดือดร้อน แต่ทำเพราะต้องการทดสอบความรู้ความสามารถของตนเอง

แครกเกอร์

Cracker

ผู้ที่แอบเข้าใช้งานระบบคอมพิวเตอร์ของหน่วยงาน หรือองค์กรอื่น โดยมีเจตนาร้ายอาจจะเข้าไปทำลายระบบ หรือสร้างความเสียหายให้กับระบบเครือข่ายขององค์กรอื่น หรือขโมยข้อมูลที่เป็นความลับทางธุรกิจ

การป้องกันภัยคุกคาม

Threat Protection

การตั้งค่ารหัสผ่าน
Password Settings

เทคโนโลยีการพิสูจน์ตัวบุคคล
Authentication Technology

การตรวจสอบและติดตาม
Monitoring and Logging

การตั้งค่าและควบคุมสิทธิ์การเข้าถึง
Access Control

การติดตั้งโปรแกรมป้องกันไวรัส
Antivirus Program

การใช้ระบบไฟร์วอลล์
Firewall System

การเข้ารหัสข้อมูล
Encryption

การสำรองข้อมูล
Back Up

การตั้งค่ารหัสผ่าน

Password Settings

เป็นการรักษาความปลอดภัยขั้นพื้นฐานในการลงชื่อเข้าสู่ระบบ การตั้งค่ารหัสผ่านที่ปลอดภัยเป็นสิ่งสำคัญ
เพื่อปกป้องข้อมูลส่วนตัวและบัญชีต่างๆ

รหัสผ่านที่ปลอดภัย

Secure Password

รหัสผ่านที่ไม่ปลอดภัย

Insecure Passwords

รหัสผ่านที่ปลอดภัย

Secure Password

- มีความยาวอย่างน้อย 8 ตัวอักษร
- มีตัวอักษรภาษาอังกฤษตัวเล็ก ตัวใหญ่
- มีอักขระพิเศษ
- ควรเปลี่ยนรหัสผ่านอยู่บ่อยๆ ครั้ง
- PIN ควรกำหนด 4 ตัวหรือ 6 ตัว ที่ไม่ง่ายต่อการคาดเดา

รหัสผ่านที่ไม่ปลอดภัย

Insecure Passwords

- ข้อมูลที่ใช้ในการระบุตัวตนทั่วไป เช่น ชื่อ นามสกุล เลขบัตรประจำตัวต่างๆ วันเดือนปีเกิด
- ข้อมูลการติดต่อ เช่น เบอร์โทรศัพท์
- ชื่อบุคคลรอบข้างหรือสัตว์เลี้ยง
- คำที่พบในพจนานุกรม
- คำทั่วๆไปที่มีการสะกดจากหลังไปหน้า เช่น

  password -> drowssap

  admin -> nimda,

  root -> toor
- ใช้รูปแบบตัวอักษรหรือตัวเลขที่เป็นที่นิยม เช่น aaabbb, qwerty, 12345, 123321
- ใช้รูปแบบการตั้งรหัสผ่านที่เหมือนหรือคล้ายคลึงกันในแต่ละบัญชี

เทคโนโลยีการพิสูจน์ตัวบุคคล

Authentication Technology

ภัยคุกคามไซเบอร์มีการแพร่หลายมากขึ้นและมีการเปลี่ยนแปลงอยู่ตลอดเวลา การกำหนดเพียงรหัสผ่านอย่างเดียวอาจไม่ปลอดภัยอีกต่อไป เราจึงจำเป็นต้องใช้มาตรการที่มีความซับซ้อนขึ้นเพื่อปกป้องตัวเราให้ปลอดภัยจากอันตราย โดยมีดังต่อไปนี้

การพิสูจน์ตัวบุคคล 2 ปัจจัย

Two-Factor Authentication

การยืนยันตัวตนด้วยชีวภาพ

Biometric Authentication

การพิสูจน์ตัวบุคคล 2 ปัจจัย

Two-Factor Authentication

เป็นการลงชื่อเข้าใช้ขั้นตอนที่ 2 หลังจากลงชื่อเข้าใช้ด้วยรหัสผ่านปกติ จะมีการยืนยันตัวตนผ่าน OTP (One-Time Password) ที่ส่งให้เราผ่านข้อความ SMS บนโทรศัพท์สมาร์ทโฟน หรือแอป Authentication เพื่อป้อนรหัสให้ตรงกัน และยืนยันตัวตน โดยรหัส OTP จะเป็นรหัสผ่านที่ใช้งานได้เพียงครั้งเดียว และมีอายุการใช้งานสั้นมาก อาจจะไม่เพียงกี่วินาที หากไม่ใช่เจ้าของบัญชี ไม่มี OTP หรือป้อนรหัสไม่ถูกต้องก็จะไม่สามารถลงชื่อเข้าใช้ได้

การยืนยันตัวตนด้วยชีวภาพ

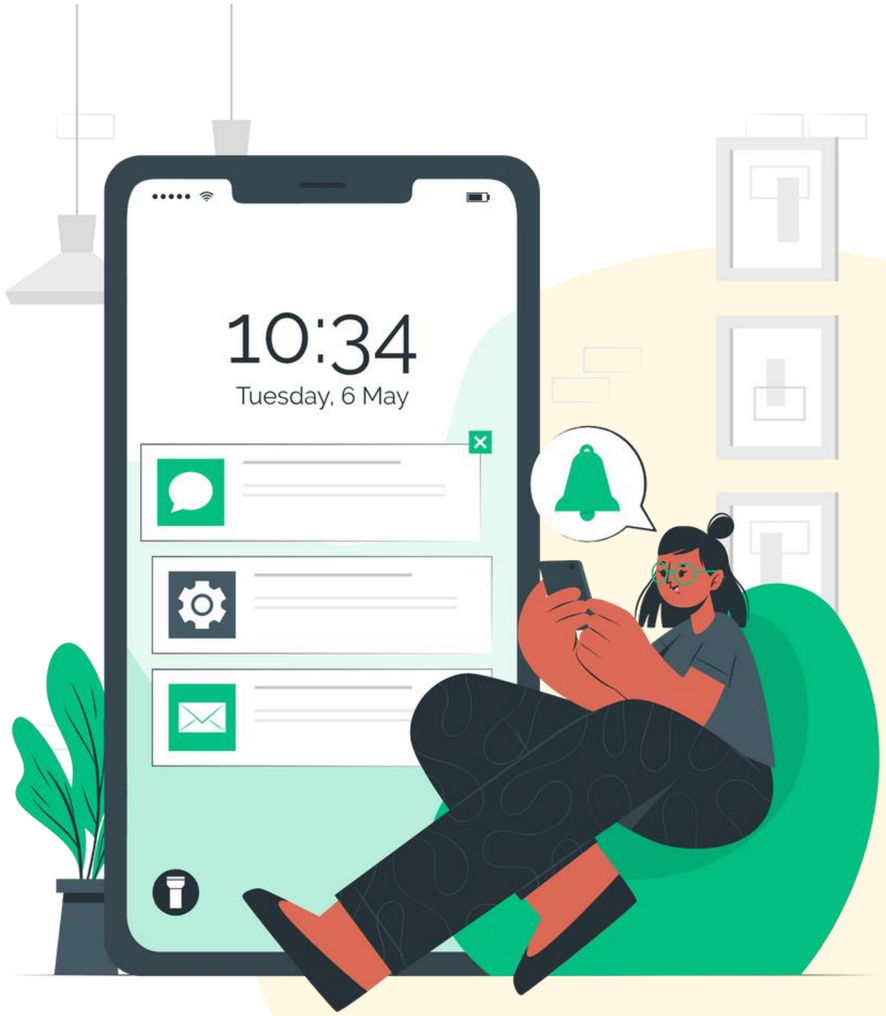
Biometric Authentication

เป็นการพิสูจน์ตัวตนเพื่อยืนยันความเป็นเจ้าของสิทธิ์การใช้งานอุปกรณ์ โดยใช้ข้อมูลทางชีวภาพที่ทุกคนบนโลกไม่เหมือนกัน เช่น การสแกนลายนิ้วมือ การสแกนม่านตา และการสแกนใบหน้า ซึ่งสิ่งเหล่านี้ไม่สามารถบอกต่อกันได้เหมือนรหัสผ่าน และใช้เวลาไม่ถึง 1 วินาทีในการเข้าใช้งานอุปกรณ์

การตรวจสอบและติดตาม

Monitoring and Logging

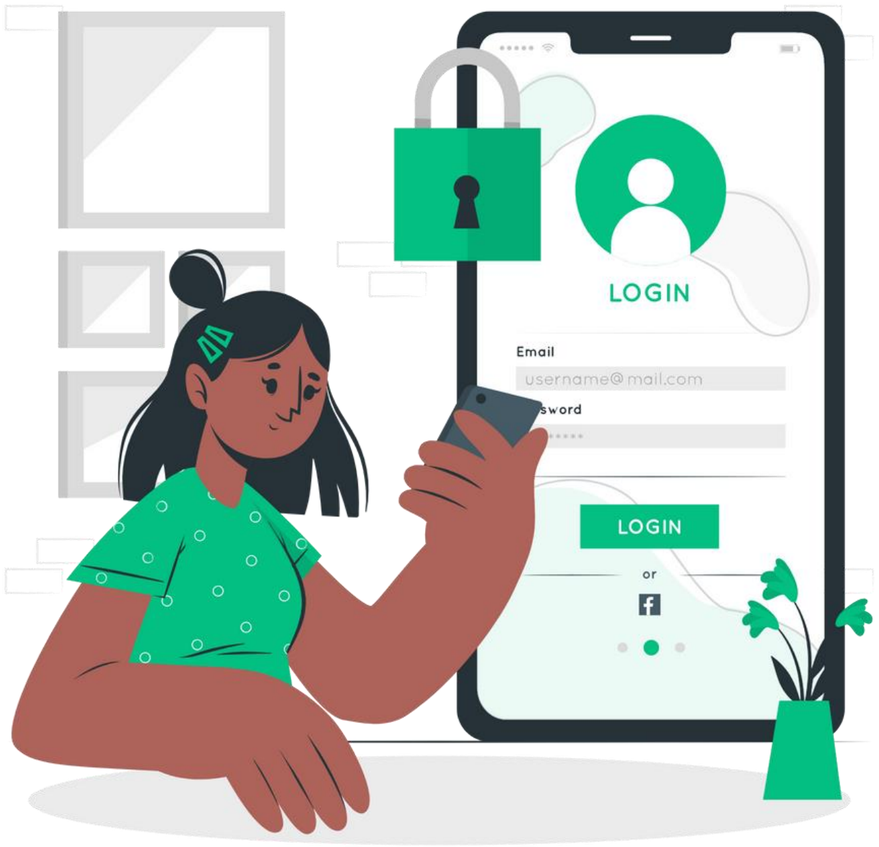
การตรวจสอบการใช้งานและบันทึกกิจกรรมช่วยให้เราสามารถตรวจพบการโจมตีหรือพฤติกรรมที่ผิดปกติได้ทันท่วงที ผู้ใช้ควรตั้งค่าการแจ้งเตือนในการใช้งานบัญชีออนไลน์ หากผู้ใช้พบความผิดปกติของการลงชื่อเข้าใช้ ระบบจะส่งการแจ้งเตือนไปยังบัญชีผู้ใช้ของเรา ทำให้เราสามารถเข้าไปตรวจสอบการลงชื่อเข้าใช้ได้ หากพบการแจ้งเตือนการลงชื่อเข้าใช้บนอุปกรณ์หรือสถานที่ที่ไม่คุ้นเคย ให้เข้าไปตรวจสอบความปลอดภัย ลงชื่อออกจากทุกอุปกรณ์ และเปลี่ยนรหัสผ่านใหม่



การตั้งค่าและควบคุมสิทธิ์การเข้าถึง

Access Control

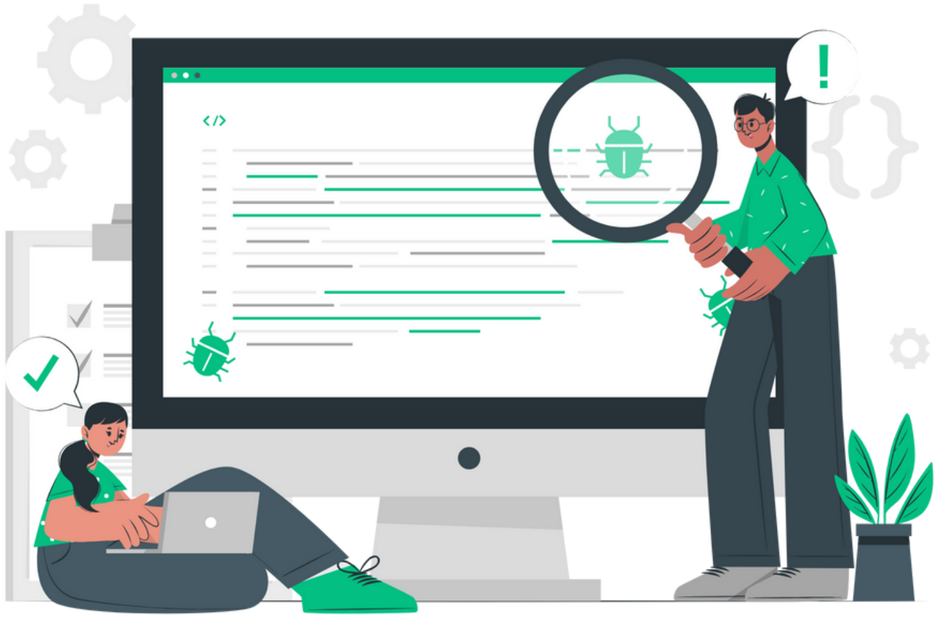
การกำหนดสิทธิ์การเข้าถึงข้อมูลและทรัพยากรต่างๆ ในระบบ ทำให้มั่นใจได้ว่ามีเฉพาะผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลสำคัญได้



การติดตั้งโปรแกรมป้องกันไวรัส

Antivirus Program

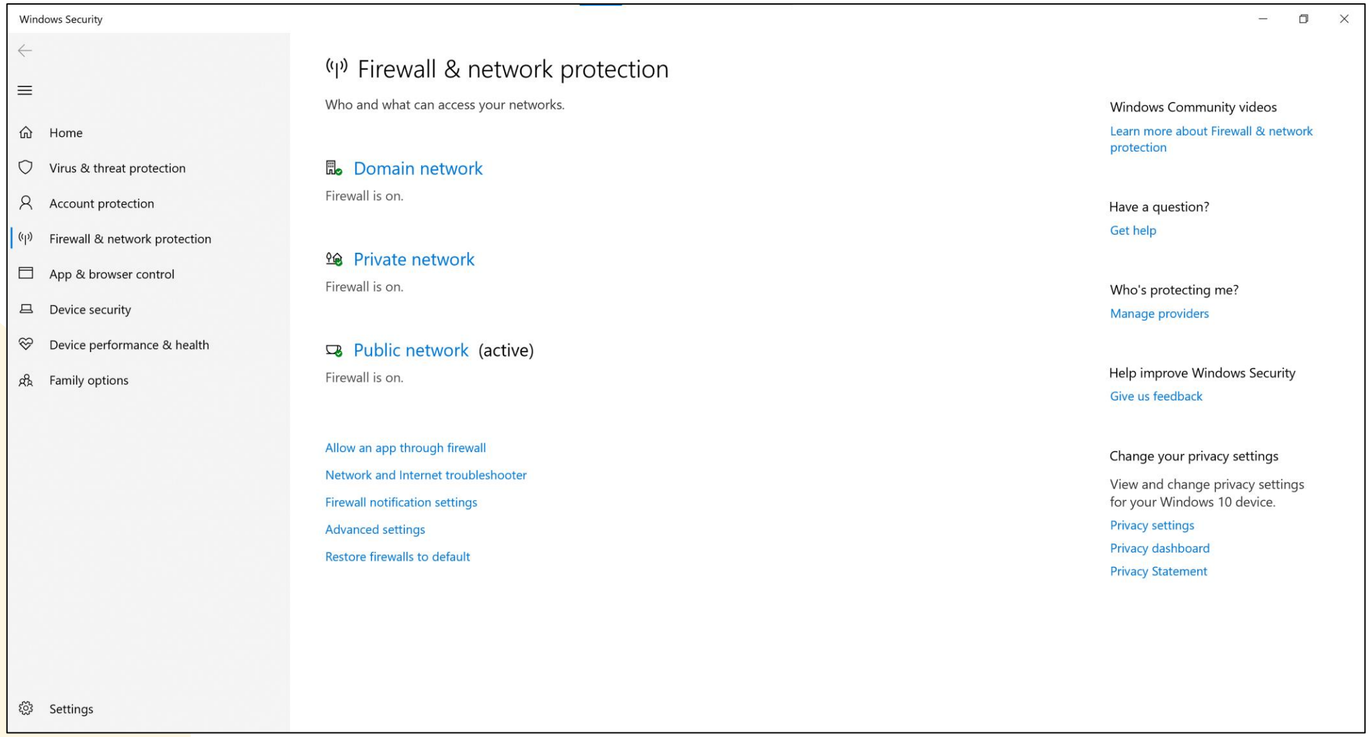
โปรแกรมป้องกันไวรัสจะทำหน้าที่คอยตรวจสอบและติดตามการบุกรุกของโปรแกรมอันตรายประเภทไวรัส หนอนอินเตอร์เน็ต และม้าโทรจัน ตลอดจนโปรแกรมประสงค์ร้ายในรูปแบบอื่นๆ โดยที่จะแจ้งเตือนให้เจ้าของเครื่องทราบได้ว่า ขณะนี้มีโปรแกรมประสงค์ร้ายใดแปลกปลอมเข้ามาและจะทำให้กำจัดหรือลบทิ้งออกไปเลยหรือไม่



การใช้ระบบไฟร์วอลล์

Firewall System

เป็นระบบรักษาความปลอดภัยที่เพื่อทำหน้าที่คอยดักจับ ป้องกันและตรวจสอบการบุกรุก รวมถึงการเข้าถึงที่ไม่ได้รับอนุญาตจากผู้ไม่ประสงค์ดีภายนอก การทำงานของระบบจะยอมให้ข้อมูลเฉพาะที่ได้รับอนุญาตผ่านเข้าออกได้เท่านั้น



การเข้ารหัสข้อมูล

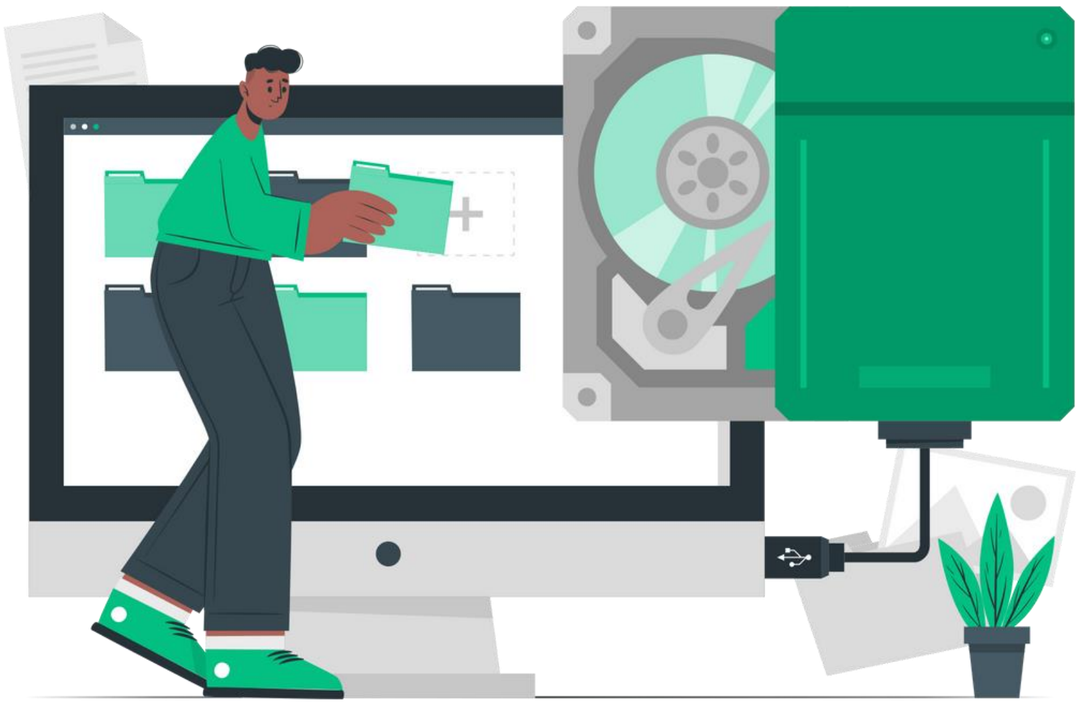
Encryption

การเข้ารหัสข้อมูล เป็นการรักษาความปลอดภัยของข้อมูลโดยอาศัยสมการทางคณิตศาสตร์ที่ซับซ้อน เพื่อทำการเปลี่ยนแปลง ข้อมูลที่อ่านได้ปกติ (Plaintext) ให้ไปอยู่ในรูปแบบของ ข้อมูลที่ไม่สามารถอ่านได้ (Ciphertext) ในการอ่านข้อมูลจำเป็นต้องถอดรหัส (Decryption) ก่อนจึงจะนำข้อมูลนั้นไปใช้ประโยชน์ได้

การสำรองข้อมูล

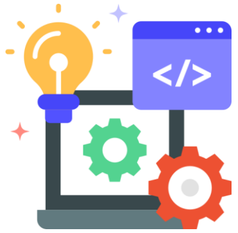
Back Up

การสำรองข้อมูล คือ การทำซ้ำข้อมูล ไฟล์ หรือโปรแกรม ไว้ในที่เก็บข้อมูลเพื่อให้สามารถนำเอากลับมาใช้ได้อีก ทั้งนี้ขึ้นอยู่กับความสำคัญของข้อมูล อาจสำรองข้อมูลเป็นรายวัน รายสัปดาห์ หรือรายเดือน



ลิขสิทธิ์ซอฟต์แวร์

Software Copyright



ความหมายของลิขสิทธิ์ซอฟต์แวร์

ประเภทของใบอนุญาตซอฟต์แวร์

การละเมิดลิขสิทธิ์ซอฟต์แวร์

ความหมายของลิขสิทธิ์ซอฟต์แวร์

ลิขสิทธิ์ซอฟต์แวร์ (Software Copyright) หมายถึง สิทธิทางกฎหมายที่มอบให้แก่ผู้สร้างสรรค์ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ เพื่อคุ้มครองผลงานของพวกเขาจากการถูกคัดลอก ใช้งาน แจกจ่าย หรือดัดแปลงโดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

ประเภทของใบอนุญาตซอฟต์แวร์

ใบอนุญาตซอฟต์แวร์ เป็นเอกสิทธิ์ที่ผู้พัฒนาซอฟต์แวร์มีสิทธิ์ควบคุมใช้ หรือเผยแพร่ได้ โดยผู้ใช้ต้องปฏิบัติตามเงื่อนไขสัญญา มี 7 ประเภท ดังนี้

1. **ซอฟต์แวร์สาธารณะ**
   Public-domain Software
2. **ซอฟต์แวร์กรรมสิทธิ์**
   Proprietary Software
3. **ซอฟต์แวร์เชิงพาณิชย์**
   Commercial Software
4. **ซอฟต์แวร์ทดลองใช้แบบจำกัดความสามารถ**
   Demo Software
5. **ซอฟต์แวร์เสรี**
   Freeware
6. **ซอฟต์แวร์ทดลองแบบจำกัดการใช้งาน**
   Shareware
7. **ซอฟต์แวร์เปิดเผยซอร์สโค้ด**
   Open-Source Software

1 ซอฟต์แวร์สาธารณะ

Public-domain Software

เป็นสัญญาอนุญาตซอฟต์แวร์ที่ไม่มีใครเป็นเจ้าของลิขสิทธิ์ หรือหมดอายุคุ้มครองสิทธิ์ไปแล้ว สามารถแก้ไข แจกจ่าย หรือจำหน่ายได้โดยไม่ต้องอ้างที่มา ส่วนใหญ่เป็นโปรแกรมที่เก่าถูกเผยแพร่ในยุคที่กฎหมายลิขสิทธิ์ยังไม่มีการคุ้มครองเรื่องซอฟต์แวร์

2 ซอฟต์แวร์กรรมสิทธิ์

Proprietary Software

ซอฟต์แวร์กรรมสิทธิ์ส่วนมากจะมีลักษณะเหมือนซอฟต์แวร์เชิงพาณิชย์ที่สามารถเช่า ซื้อ หรือขายLicense ผู้ซื้อสามารถใช้งานฟีเจอร์ต่างๆ ได้ตามต้องการ และจะไม่เปิดเผย Source Code ให้แก่ผู้ใช้งาน เช่น WinRAR, Skype และ Windows

3 ซอฟต์แวร์เชิงพาณิชย์

Commercial Software

เป็นซอฟต์แวร์ที่จัดทำเพื่อขายหรือวัตถุประสงค์การค้าเท่านั้น ผู้ซื้อสามารถเช่าหรือซื้อได้ที่ตัวแทนจำหน่ายและผู้พัฒนา โดยผู้พัฒนามักจะออกแบบเงื่อนไขในการใช้งานจำกัดจำนวนผู้ใช้งาน และจำกัดฟีเจอร์บางอย่างเป็นต้น เช่น Microsoft 365 และแบ่งแพ็คเกจการใช้งานเช่น สำหรับคนทั่วไป สำหรับใช้ในองค์กร สำหรับใช้ในสถานศึกษา

4 ซอฟต์แวร์ทดลองใช้แบบจำกัดความสามารถ

Demo Software

เป็นซอฟต์แวร์ที่เปิดให้ทดลองใช้ ไม่จำกัดเวลา แต่บางฟังก์ชันอาจจะยังไม่เปิดใช้งาน ซึ่งยังสามารถใช้งานฟังก์ชันหลักได้ เช่น Daemon Tool และ CCleaner เป็นต้น

5 ซอฟต์แวร์เสรี

Freeware

เป็นซอฟต์แวร์ลิขสิทธิ์ที่ให้ดาวน์โหลดฟรี ผู้ใช้จะไม่มีสิทธิ์ในการดัดแปลง แก้ไข หรือขายซอฟต์แวร์ โดยส่วนใหญ่จะเป็นโปรแกรมที่มักทำออกมาเพื่อจูงใจให้ผู้ใช้ต้องการซื้อในเวอร์ชั่นที่จะต้องเสียเงินเช่น โปรแกรม Anti-Virus, โปรแกรม GOM Player

6 ซอฟต์แวร์ทดลอง แบบจำกัดการใช้งาน

Shareware

เป็นโปรแกรมคอมพิวเตอร์ที่ถูกพัฒนาอยู่กึ่งกลางระหว่าง Freeware และ Commercial มีลักษณะคล้ายกับ Demo แตกต่างกันในส่วนที่มีเงื่อนไขเรื่องระยะเวลา เช่น จำนวนวันใช้งาน, มีฟังก์ชันไม่ครบ และอาจจะมีโฆษณาเข้ามากวนใจด้วย

7 ซอฟต์แวร์เปิดเผยซอร์สโค้ด

Open-Source Software

เป็นซอฟต์แวร์ที่ให้ใช้งานฟรีเหมือนกับ Freeware ผู้ใช้งานสามารถปรับปรุง แก้ไข โค้ดของโปรแกรมคอมพิวเตอร์ประเภทนี้ได้ โดยอยู่ภายใต้สัญญาอนุญาตเดียวกับซอฟต์แวร์ต้นฉบับ เช่น ระบบปฏิบัติการ Linux, 7-Zip และ FileZilla เป็นต้น

การละเมิดลิขสิทธิ์ซอฟต์แวร์

การละเมิดลิขสิทธิ์ทางตรง

Direct Copyright Infringement

การละเมิดลิขสิทธิ์ทางอ้อม

Indirect Copyright Infringement

การละเมิดลิขสิทธิ์ทางตรง

(Direct Copyright Infringement

เป็นการทำซ้ำ ดัดแปลง เผยแพร่โปรแกรมคอมพิวเตอร์แก่สาธารณชน รวมทั้งการนำต้นฉบับหรือสำเนางานดังกล่าวออกให้เช่า โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

การละเมิดลิขสิทธิ์ทางอ้อม

Indirect Copyright Infringement

เป็นการกระทำทางการค้า หรือการกระทำที่มีส่วนสนับสนุนให้เกิดการละเมิดลิขสิทธิ์ดังกล่าวข้างต้นโดยผู้กระทำรู้อยู่แล้ว ว่างานใดได้ทำขึ้นโดยละเมิดลิขสิทธิ์ของผู้อื่น แต่ก็ยังกระทำเพื่อหากำไรจากงานนั้น ได้แก่ การขาย มีไว้เพื่อขาย ให้เช่า เสนอให้เช่า ให้เช่าซื้อ เสนอให้เช่าซื้อ เผยแพร่ต่อสาธารณชน แจกจ่ายในลักษณะที่อาจก่อให้เกิดความเสียหายต่อเจ้าของลิขสิทธิ์และนำหรือสั่งเข้ามาในราชอาณาจักร

จริยธรรมในการใช้เทคโนโลยีสารสนเทศ

Information Technology Ethics

เป็นหลักศีลธรรมจรรยาที่กำหนดขึ้นเพื่อใช้เป็นแนวทางปฏิบัติ หรือควบคุมการใช้ระบบคอมพิวเตอร์และสารสนเทศ

ประกอบด้วย 4 ประเด็น เรียกย่อๆ ว่า PAPA

ความเป็นส่วนตัว

Privacy

ความถูกต้อง

Accuracy

ความเป็นเจ้าของ

Property

การเข้าถึงข้อมูล

Accessibility

ความเป็นส่วนตัว

Privacy

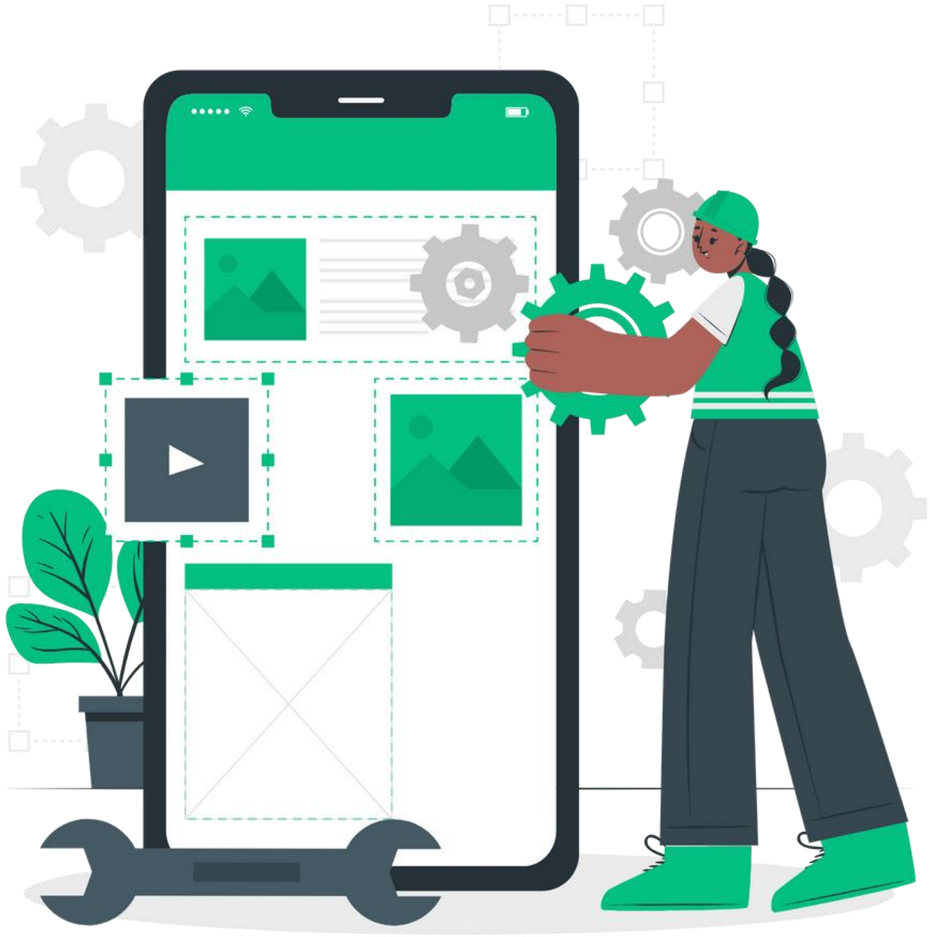
สิทธิที่จะอยู่ตามลำพัง และเป็นสิทธิที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น สิทธินี้ใช้ได้ครอบคลุมทั้งตัวบุคคล กลุ่มบุคคล และองค์กรต่างๆ ซึ่งการละเมิดความเป็นส่วนตัวเช่น การดูข้อมูลในคอมพิวเตอร์ หรือการแอบเข้าไปดูข้อความใน E-Mail ของบุคคลอื่น

ความถูกต้อง

Accuracy

เป็นการใช้คอมพิวเตอร์เพื่อการรวบรวม จัดเก็บ และเรียกใช้ข้อมูล มีลักษณะดังนี้

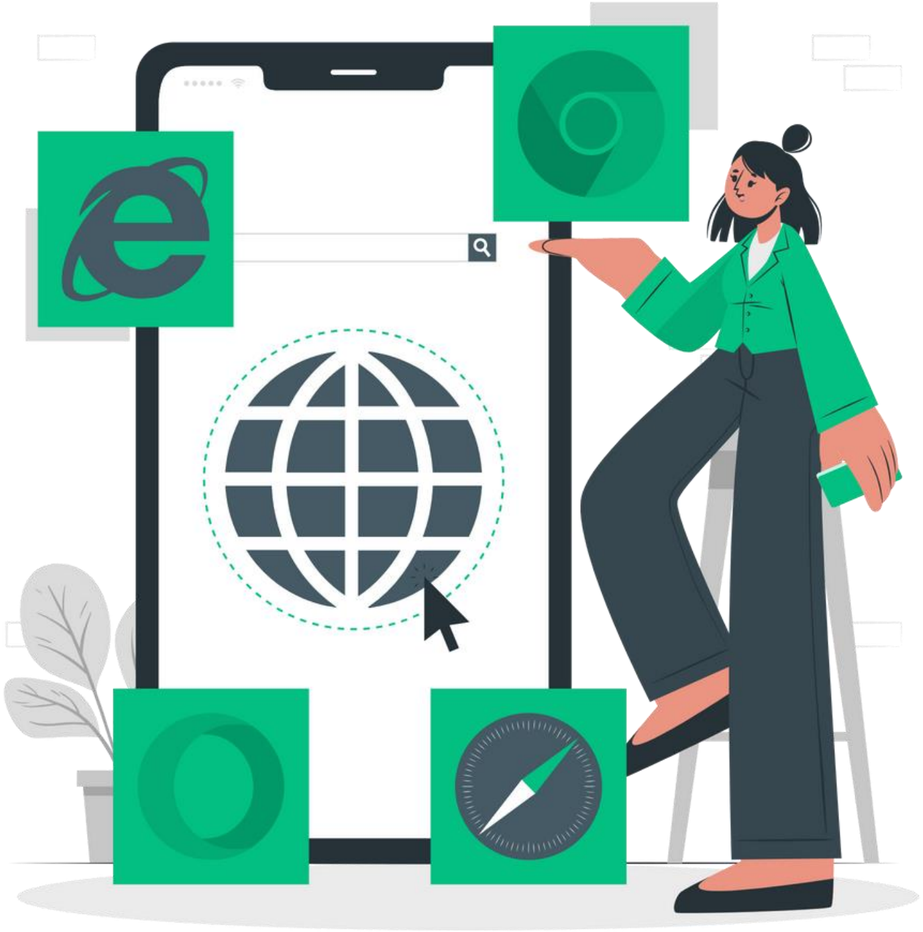
1. การบันทึกข้อมูลมีความถูกต้องตามข้อเท็จจริง
2. มีผู้รับผิดชอบในเรื่องความถูกต้องของข้อมูลที่จัดเก็บและเผยแพร่
3. มีการตรวจสอบความถูกต้องของข้อมูลก่อนการบันทึกหรือนำเข้าฐานข้อมูล
4. มีการปรับปรุงให้มีความทันสมัยอยู่เสมอ
5. ควรให้สิทธิแก่บุคคลในการเข้าไปตรวจสอบความถูกต้องของข้อมูลของตนเองได้



ความเป็นเจ้าของ

Property

กรรมสิทธิ์ในการถือครองทรัพย์สิน อาจเป็นทรัพย์สินที่จับต้องได้ เช่น อุปกรณ์คอมพิวเตอร์ หรืออาจเป็นทรัพย์สินจับต้องไม่ได้ เช่น ดนตรี วรรณกรรม โปรแกรมและคอมพิวเตอร์ ซึ่งการจัดเก็บในรูปแบบดิจิทัล ทำให้ง่ายต่อการคัดลอกและนำไปใช้โดยไม่ได้รับอนุญาตจากเจ้าของผลงาน จึงเกิดเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาขึ้น



การเข้าถึงข้อมูล

Accessibility

เป็นแนวปฏิบัติในการเข้าใช้งานข้อมูล โปรแกรม หรือระบบคอมพิวเตอร์ การรักษาความลับและความปลอดภัยของข้อมูล จะต้องมีการกำหนดสิทธิการเข้าถึงข้อมูลตามระดับของผู้ใช้งาน และป้องกันมิให้ผู้ใช้ที่ไม่ส่วนเกี่ยวข้องเข้าดำเนินการต่างๆ กับข้อมูล การเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอมนั้น ถือเป็นการผิดจริยธรรมเช่นเดียวกับการละเมิดข้อมูลส่วนตัว

จรรยาบรรณผู้ใช้เทคโนโลยีสารสนเทศ

1. ต้องไม่ใช้คอมพิวเตอร์ทำร้ายหรือละเมิดผู้อื่น
2. ต้องไม่รบกวนการทำงานของผู้อื่น
3. ต้องไม่สอดแนมหรือแก้ไขเปิดดูในแฟ้มของผู้อื่น
4. ต้องไม่ใช้คอมพิวเตอร์เพื่อการโจรกรรมข้อมูลข่าวสาร
5. ต้องไม่ใช้คอมพิวเตอร์สร้างหลักฐานที่เป็นเท็จ
6. ต้องไม่คัดลอกโปรแกรมผู้อื่นที่มีลิขสิทธิ์
7. ต้องไม่ละเมิดการใช้ทรัพยากรคอมพิวเตอร์โดยที่ตนเองไม่มีสิทธิ์
8. ต้องไม่นำเอาผลงานของผู้อื่นมาเป็นของตน
9. ต้องคำนึงถึงสิ่งที่จะเกิดขึ้นกับสังคมอันติดตามมาจากการกระทำ
10. ต้องใช้คอมพิวเตอร์โดยเคารพกฎระเบียบ กติกา และมารยาท

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
5	ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน	0.5	10,000
6	ผู้ใดล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะ ถ้านำมาตรการดังกล่าวไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น	1	20,000
7	ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน	2	40,000
8	ผู้ใดกระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้	3	60,000

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
9	ผู้ใดทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ	5	100,000
10	ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้	5	100,000
11	ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข		100,000
	ผู้ใดส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นอันมีลักษณะเป็นการก่อให้เกิดความเดือดร้อนรำคาญแก่ผู้รับข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ โดยไม่เปิดโอกาสให้ผู้รับสามารถบอกเลิกหรือแจ้งความประสงค์เพื่อปฏิเสธการตอบรับได้โดยง่าย		200,000

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
12	ถ้าการกระทำผิดตามมาตรา 5, 6, 7, 8 หรือ 11 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ	1 ถึง 7	20,000 ถึง 140,000
	ถ้าการกระทำผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว	1 ถึง 10	20,000 ถึง 200,000
	ถ้าการกระทำผิดตามมาตรา 9 หรือ 10 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง	3 ถึง 15	60,000 ถึง 300,000
	ถ้าการกระทำผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย	5 ถึง 20	100,000 ถึง 400,000

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
12/1	ถ้าการกระทำผิดตามมาตรา 7 หรือ 10 เป็นเหตุให้เกิดอันตรายแก่บุคคลหรือทรัพย์สินของผู้อื่น	10	200,000
	ถ้าการกระทำความผิดตามมาตรา 9 หรือ 10 โดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย	5 ถึง 20	100,000 ถึง 400,000
13	ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามมาตรา 5, 6, 7, 8, 9, 10 หรือ 11	1	20,000
	ผู้ใดจำหน่ายหรือเผยแพร่ชุดคำสั่งที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตามาตรา 12 วรรคหนึ่งหรือวรรคสาม	2	40,000

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
14	ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้	5	100,000
	1. ผู้ใดกระทำความผิดโดยทุจริต หรือโดยหลอกลวง นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมไม่ว่าทั้งหมดหรือบางส่วน หรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ประชาชน อันมิใช่ การกระทำผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา		
	2. ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะของประเทศ หรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน		

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
14	ผู้ใดกระทำความผิดที่ระบุไว้ดังต่อไปนี้	5	100,000
	3. ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา		
	4. ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้		
	5. ผู้ใดเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) หรือ (4)		
15	ผู้ให้บริการผู้ใดให้ความร่วมมือ ยินยอม หรือรู้เห็นเป็นใจให้มีการกระทำความผิดตามมาตรา 14 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน	5	100,000

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
16	ผู้ใดนำเข้าสู่ระบบคอมพิวเตอร์ที่ประชาชนทั่วไปอาจเข้าถึงได้ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย • ถ้าการกระทำตามวรรคหนึ่งเป็นการกระทำต่อภาพของผู้ตาย และการกระทำนั้นน่าจะทำให้บิดา มารดา คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ถูกดูหมิ่น หรือถูกเกลียดชัง หรือได้รับความอับอาย ผู้กระทำต้องระวางโทษดังที่บัญญัติไว้ในวรรคหนึ่ง • ถ้าการกระทำตามวรรคหนึ่งหรือวรรคสอง เป็นการนำเข้าสู่ระบบคอมพิวเตอร์โดยสุจริตอันเป็นการติชมด้วยความเป็นธรรม ซึ่งบุคคลหรือสิ่งใดอันเป็นวิสัยของประชาชนย่อมกระทำ ผู้กระทำไม่มีความผิด • ความผิดตามวรรคหนึ่งและวรรคสองเป็นความผิดอันยอมความได้ • ถ้าผู้เสียหายในความผิดตามวรรคหนึ่งหรือวรรคสองตายเสียก่อนร้องทุกข์ ให้บิดา มารดา คู่สมรส หรือบุตรของผู้เสียหายร้องทุกข์ได้ และให้ถือว่าเป็นผู้เสียหาย	3	200,000

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
16/1	ในคดีความผิดตามมาตรา 14 หรือ16 ซึ่งมีคำพิพากษาว่าจำเลยมีความผิด ศาลอาจสั่ง (1) ให้ทำลายข้อมูลตามมาตราดังกล่าว (2) ให้โฆษณาหรือเผยแพร่คำพิพากษาทั้งหมดหรือแต่บางส่วนในสื่ออิเล็กทรอนิกส์ วิทยุกระจายเสียง วิทยุโทรทัศน์ หนังสือพิมพ์ หรือสื่ออื่นใดตามที่ศาลเห็นสมควร โดยให้จำเลยเป็นผู้ชำระค่าโฆษณาหรือเผยแพร่ (3) ให้ดำเนินการอื่นตามที่ศาลเห็นสมควรเพื่อบรรเทาความเสียหายที่เกิดขึ้นจากการกระทำความผิดนั้น		
16/2	ผู้ใดรู้ว่าข้อมูลคอมพิวเตอร์ในความครอบครองของตนเป็นข้อมูลที่ศาลสั่งให้ทำลายตามมาตรา 16/1 ผู้นั้นต้องทำลายข้อมูลดังกล่าว หากฝ่าฝืนต้องระวางโทษกึ่งหนึ่งของโทษที่บัญญัติไว้ในมาตรา 14 หรือ 16 แล้วแต่กรณี		

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
17	ผู้ใดกระทำความผิดตามพระราชบัญญัตินี้นอกราชอาณาจักรและ (1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้นหรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ (2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหายและผู้เสียหายได้ร้องขอให้ลงโทษ จะต้องรับโทษภายในราชอาณาจักร		
17/1	ความผิดตามมาตรา 5, 6, 7, 11, 13 วรรคหนึ่ง, 16/2, 23, 24 และ 27 ให้คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งมีอำนาจเปรียบเทียบได้ • คณะกรรมการเปรียบเทียบที่รัฐมนตรีแต่งตั้งตามวรรคหนึ่งให้มีจำนวนสามคนซึ่งคนหนึ่งต้องเป็นพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา • เมื่อคณะกรรมการเปรียบเทียบได้ทำการเปรียบเทียบกรณีใดและผู้ต้องหาได้ชำระเงินค่าปรับตามคำเปรียบเทียบภายในระยะเวลาที่คณะกรรมการเปรียบเทียบกำหนดแล้ว ให้ถือว่าคดีนั้นเป็นอันเลิกกันตามประมวลกฎหมายวิธีพิจารณาความอาญา		

กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 รายละเอียดของบทลงโทษและค่าปรับ มีดังนี้

มาตรา	การกระทำความผิด	จำคุกไม่เกิน (ปี)	ค่าปรับไม่เกิน (บาท)
17/1	• ในกรณีที่ผู้ต้องหาไม่ชำระเงินค่าปรับภายในระยะเวลาที่กำหนด ให้เริ่มนับอายุความในการฟ้องคดีใหม่นับตั้งแต่วันที่ครบกำหนดระยะเวลาดังกล่าว		