

สพม.พะเยา

คู่มือรู้เท่าทันสื่อและเทคโนโลยี เพื่อป้องกันภัยไซเบอร์ สำหรับการดำเนินชีวิตวิถีใหม่และวิถีถัดไป

เอกสารประกอบการจัดการความรู้
[KNOWLEDGE MANAGEMENT]



กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพะเยา
สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน
กระทรวงศึกษาธิการ

คู่มือรู้เท่าทันสื่อและเทคโนโลยีเพื่อป้องกันภัยไซเบอร์ สำหรับการดำเนินชีวิตวิถีใหม่และวิถีถัดไป

รวบรวมโดย กลุ่มส่งเสริมการศึกษาทางไกล เทคโนโลยีสารสนเทศและการสื่อสาร
สำนักงานเขตพื้นที่การศึกษามัธยมศึกษาพะเยา

บทนำ

การใช้เทคโนโลยีอย่างรู้เท่าทัน

ที่มา website คลังความรู้ Scimath <https://www.scimath.org/>

ในชีวิตประจำวันของเรา เทคโนโลยีสารสนเทศมีบทบาทกับการดำเนินชีวิตในปัจจุบันเป็นอย่างมาก ในขณะที่ในทุก ๆ วันเทคโนโลยีมีการเปลี่ยนแปลงตลอดเวลา เราเองก็ต้องเรียนรู้และปรับตัวให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยี อย่างไรก็ตาม เทคโนโลยีนั้นมิทั้งคุณประโยชน์และโทษในเวลาเดียวกัน เพื่อให้เรามีความรู้และสามารถใช้เทคโนโลยีได้อย่างมีประสิทธิภาพและปลอดภัย ก็จำเป็นที่จะต้องมีความรู้เกี่ยวกับความรู้ทางด้านต่าง ๆ ต่อไปนี้

1. การรู้เท่าทันสื่อ
2. แนวทางการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัยและมีจริยธรรม
3. การรักษาข้อมูลส่วนตัว
4. การรับมือการคุกคามทางออนไลน์
5. ลิขสิทธิ์และความเป็นเจ้าของผลงาน
6. กฎหมายเกี่ยวกับคอมพิวเตอร์และการกระทำความผิดทางคอมพิวเตอร์

1. การรู้เท่าทันสื่อ

แนวคิดการรู้เท่าทันสื่อถือกำเนิดขึ้นพร้อมกับความก้าวหน้าของเทคโนโลยีทางการสื่อสารที่เกิดขึ้นกับสื่อต่าง ๆ ตั้งแต่ยุคของสื่อวิทยุกระจายเสียง วิทยุโทรทัศน์ในระบบแอนะล็อก(Analog) จนก้าวมาสู่ยุคสารสนเทศที่สื่อต่าง ๆ สื่อสารผ่านระบบดิจิทัล อันเป็นยุคที่สื่อต่าง ๆ ถูกหลอมรวมเข้าหากัน ความก้าวหน้าของเทคโนโลยีในการสื่อสารที่ทำให้ผู้คนไม่ว่าจะอยู่มุมใดของโลกสามารถที่จะเข้าถึงข้อมูลข่าวสารได้นั้นในอีกแง่หนึ่งที่ไม่สามารถปฏิเสธได้ก็คือความก้าวหน้าของเทคโนโลยีการสื่อสารเหล่านี้ได้เพิ่มอำนาจให้กับผู้ส่งสารซึ่งมักจะเป็นองค์กรสื่อสารมวลชนขนาดใหญ่มีเงินทุนจำนวนมากที่มีผู้คนเพียงไม่กี่รายที่จะสามารถเข้าถึงกรรมสิทธิ์ความเป็นเจ้าของสื่อ และขับเคลื่อนไปด้วยปัจจัยทางเศรษฐกิจ ระบบการสื่อสารจากที่อำนาจไปกระจุกตัวอยู่ที่ผู้ส่งสารให้ถ่ายเทมาอยู่ในฝั่งผู้รับสารด้วยการปลูกฝังแนวคิดการรู้เท่าทันสื่อ อันเป็นการเปลี่ยนแปลงทางสังคมจนนำไปสู่การตระหนักถึงความสำคัญของการติดตั้งกลไกการรู้เท่าทันสื่อ

จึงเกิดคำถามตามมาว่า จะเกิดอะไรขึ้นหากประชาชนผู้บริโภคเนื้อหาข้อมูลข่าวสาร โดยเฉพาะเด็กและเยาวชน เสพสารนั้นโดยไม่วิเคราะห์ให้ถี่ถ้วนกับเนื้อหาข้อมูล ปริมาณมหาศาลที่สื่อนำเสนอ จากสภาพในเมื่อทุกคนไม่สามารถหลีกเลี่ยงฐานะของผู้รับสารที่ต้องเผชิญกับรับข้อมูล ข่าวสารจำนวนมากที่สื่อนำเสนอมาด้วยวัตถุประสงค์ต่าง ๆ การรู้เท่าทันสื่อจึงเป็นกลไกที่สำคัญและจำเป็น ดังนั้นเราต้องปกป้องตัวของเรา

โดยต้องรู้ให้เท่าทันสื่อ เพราะถ้าเราเลือกที่จะไม่เปิดรับสารและสื่อเลย เราก็อาจจะพลาดข้อมูลที่สำคัญสำหรับการดำรงชีวิตของเราได้หรือถ้าเราเปิดรับสารและสื่อที่ไม่มีประโยชน์ต่อตัวของเรา ก็จะเกิดผลกระทบในทางลบมากกว่าทางบวก ผลที่ตามมาจากการไม่รู้เท่าทันสื่อ คือ การที่ผู้รับสารสูญเสียการรับรู้โลกที่เป็นจริง แต่จะรับรู้โลกผ่านสายตาสื่อแต่เพียงอย่างเดียว นั้นย่อมหมายถึงผู้รับสารกำลังยอมรับทุกอย่างที่สื่อบอก โดยปราศจากการตั้งคำถาม ต่อรอง ต่อต้าน นิยาม การเล่าเรื่องราว การสร้างภาพตัวแทนของสิ่งต่าง ๆ ผ่านสายตาสื่อมนุษย์จึงจำเป็นต้องมีความสามารถในการรู้เท่าทันสื่อเพื่อใช้รับมือกับสื่อที่มีแพร่หลายในปัจจุบัน โดยความสามารถในการรู้เท่าทันสื่อ มี 4 องค์ประกอบ ดังนี้

1. ความสามารถในการเข้าถึงสื่อและสาร คือ ความสามารถในการแสวงหาแหล่งที่มา การเลือกและการจัดการ การคัดกรอง การถอดรหัสของข้อมูลข่าวสารในสื่อประเภทต่างๆ รวมถึงความสามารถในการใช้สื่อและเทคโนโลยีต่างๆ เช่น สิ่งพิมพ์ วิดีโอ คอมพิวเตอร์ และอินเทอร์เน็ต

2. ความสามารถในการวิเคราะห์สื่อและสาร คือ ความสามารถในการเข้าใจสื่อและเนื้อหาสาร สามารถตีความ จัดประเภท กำหนดรูปแบบของงาน โดยใช้การวิเคราะห์และอนุมานเหตุและผล ซึ่งอาศัยพื้นฐานความรู้เดิม ประสบการณ์ และการตัดสินใจเกี่ยวกับสื่อและเนื้อหาสาร รวมถึงความสามารถในการบอกจุดประสงค์ของผู้ผลิตสื่อได้

3. ความสามารถในการประเมินสื่อและสาร คือ ความสามารถในการตัดสินใจคุณค่าและความมีประโยชน์ของสารต่อผู้รับสาร โดยใช้การประเมินสื่อและสารยึดหลักคุณธรรม จริยธรรมในตนเอง และยังอาศัยพื้นฐานความรู้เดิมที่มีมาแปลความหมายของสาร รวมถึงการระบุค่านิยมและคุณค่าของสาร และชื่นชมคุณภาพของงานในเชิงสุนทรีย์ทางศิลปะ

4. ความสามารถในการสร้างสรรค์สื่อและสาร คือ ความสามารถในการเข้าใจและตระหนักรู้ถึงความสนใจของผู้รับสาร โดยสามารถสร้างสารที่เป็นรูปแบบของตนเองจากเครื่องมือและสื่อที่หลากหลาย โดยใช้การจัดลำดับขั้นของความคิด การใช้สัญลักษณ์ในการสื่อสาร และใช้ทักษะการผลิตสื่อ เช่น การทบทวนแก้ไข การพิมพ์ การผลิตและตัดต่อวิดีโอ การพูด เป็นต้น

นอกจากนี้ Center for Media Literacy ยังได้แนะนำกรอบทักษะที่ชื่อว่า “Process Skills: Success for Life” อันเป็นข้อเสนอแนะเกี่ยวกับทักษะที่เยาวชนจะต้องมีในการก้าวเข้าสู่ศตวรรษที่ 21 ในรายงานเรื่อง Learning for the 21st Century ซึ่งพัฒนาโดยผู้นำองค์กรเอกชนและนักการศึกษา ภายใต้กรอบแนวคิด CML MediaLit KitTM ที่ผู้เรียนจะไม่เพียงแต่เพิ่มความรู้เกี่ยวกับเนื้อหาสาระของสื่อในปัจจุบันเท่านั้น แต่ผู้เรียนจะต้องเรียนรู้และปฏิบัติทักษะดังต่อไปนี้ได้

1. การเข้าถึง เป็นทักษะที่ผู้เรียนสามารถที่จะเก็บข้อมูลที่เกี่ยวข้อง และใช้ประโยชน์จากข้อมูลนั้น ตลอดจนทำความเข้าใจความหมาย กล่าวคือ ผู้เรียนสามารถที่จะจดจำ เข้าใจศัพท์ต่าง ๆ สัญลักษณ์เทคนิคในการสื่อสารรู้จักจัดแบ่งประเภทของข้อมูลตามจุดประสงค์ของงาน

2. การวิเคราะห์ เป็นทักษะที่ผู้เรียนสามารถที่จะพิจารณาการออกแบบรูปแบบของเนื้อหาสื่อ โครงสร้าง สามารถใช้แนวคิดในด้านศิลปะ วรรณกรรม สังคม การเมือง เศรษฐกิจในการทำความเข้าใจบริบทที่เนื้อหาข่าวสารนั้นถูกสร้างขึ้น เช่น การใช้ความรู้ ประสบการณ์ที่มีทำนายผลลัพธ์ที่จะเกิดขึ้น ตีความข่าวสารโดยใช้แนวคิดเกี่ยวกับจุดประสงค์ ผู้รับสาร มุมมอง รูปแบบ ประเภท บุคลิกลักษณะ โครงเรื่อง แก่นเรื่อง

อารมณ์ ฉาก และบริบท ใช้กลยุทธ์ต่าง ๆ ไม่ว่าจะเป็น การเปรียบเทียบ การขัดแย้ง การให้ข้อเท็จจริง ความคิดเห็น เหตุและผล การเรียงลำดับ และผลที่ตามมา

3. การประเมิน เป็นทักษะที่ผู้เรียนสามารถที่จะเชื่อมโยงเนื้อหาสารกับประสบการณ์ของพวกเขาและตัดสินความถูกต้อง คุณภาพ ความเกี่ยวข้องของเนื้อหาสาร เช่น สามารถชื่นชม มีความพึงพอใจในการตีความเนื้อหาสารที่มีประเภท และรูปแบบที่แตกต่างกัน ประเมินคุณภาพของเนื้อหาสารจากเนื้อหาและรูปแบบ ตัดสินคุณค่าของเนื้อหาสารจากจากหลักทางศีลธรรม ศาสนา และหลักการประชาธิปไตย สามารถที่จะโต้ตอบ ไม่ว่าจะเป็นโดยการเขียน การพิมพ์ ทางอิเล็กทรอนิกส์ต่อเนื้อหาสารที่มีความซับซ้อนอันหลากหลาย

4. สร้างสรรค์ เป็นทักษะในการเขียนแสดงออกถึงความคิดสร้างสรรค์ การใช้คำ ใช้เสียง และภาพอย่างมีประสิทธิภาพเพื่อจุดประสงค์อันหลากหลาย สามารถใช้เทคโนโลยีในการสร้างสรรค์ ตัดต่อ และแพร่กระจายเนื้อหา เช่น การระดมความคิด การวางแผน การวางแผนและทบทวนกระบวนการ การใช้ภาษาพูด และเขียนอย่างมีประสิทธิภาพ เชี่ยวชาญในกฎของการใช้ภาษา สร้างและเลือกภาพได้อย่างมีประสิทธิภาพ เพื่อให้เป้าหมายอย่างหลากหลาย ใช้เทคโนโลยีการสื่อสารในการสร้างเนื้อหาสาร เป็นต้น

กรอบในการเรียนรู้การรู้เท่าทันสื่อ โดยการถามผู้เรียนด้วยกรอบคำถาม 5 คำถาม ได้แก่

1. ใครเป็นผู้ส่งสารนี้ และจุดประสงค์ของผู้พูดคืออะไร
2. เทคนิคอะไรที่ถูกใช้ในการดึงดูดความสนใจ
3. วิถีชีวิต ค่านิยม มุมมองแบบไหนที่ถูกนำเสนอในสารนี้
4. ผู้รับสารที่แตกต่างกันตีความสารนี้แตกต่างกันอย่างไร
5. อะไรบ้างที่ถูกกลบเกล็นในสารนี้

ชุดคำถามทั้ง 5 คำถาม จะถูกนำไปใช้ในการวิเคราะห์สื่อในรูปแบบต่าง ๆ 4 รูปแบบ คือ โฆษณา การชักจูงใจและการโฆษณาชวนเชื่อการวิเคราะห์การเล่าเรื่องในสื่อบันเทิงต่าง ๆ และภาพตัวแทนของเพศ เชื้อชาติ และอุดมการณ์ต่าง ๆ ที่ปรากฏในเนื้อหาสื่อ ตัวอย่างแนวทางในการวิเคราะห์ เช่น การเปรียบเทียบเนื้อหาของเรื่องเล่าในสื่อที่แตกต่างกัน การวิเคราะห์ภาพตัวแทนของชายและหญิงในสื่อโฆษณา เทคนิควิธีที่ถูกใช้ในสื่อสิ่งพิมพ์ การศึกษาเนื้อหาสื่อแบบสารคดีในสื่อสิ่งพิมพ์

การรู้เท่าสื่อจึงมีความสำคัญมากในฐานะทักษะและความสามารถของผู้เรียนในศตวรรษที่ 21 ที่สามารถเลือกรับวิเคราะห์ ข้อมูล ข่าวสาร โดยเฉพาะสื่อที่ส่งผ่านช่องทางอินเทอร์เน็ต หรือสื่อสังคมออนไลน์ พิจารณาโดยตั้งคำถามกับสื่อที่เราเลือกรับ การประเมินสื่อเราสารโดยยึดหลักคุณธรรม จริยธรรม เราก็จะไม่ตกเป็นเหยื่อของสื่อ นั้น

แหล่งที่มา

ชนัญสรุ อรณพ ณ อยุธยา. (2560). การรู้เท่าทันการสื่อสารกับการขับเคลื่อนวาระปฏิรูปสังคมไทยในยุคดิจิทัล. สุทธิปริทัศน์, 31 (97), 21-33.

นิตยา วงศ์ใหญ่. (2560,พฤษภาคม). แนวทางการพัฒนาทักษะการรู้ดิจิทัลของดิจิทัลเนทีฟ.Veridian E-Journal Silpakorn University, 10 (2), 1630-1642.

ปณิดา วรณพิรุณ. (2560). ความฉลาดทางดิจิทัล. พัฒนาเทคนิคศึกษา, 29 (102), 12-20.

วิทยา ดำรงเกียรติศักดิ์. (2558). พลเมืองดิจิทัล. เชียงใหม่: คณะสารสนเทศและการสื่อสาร มหาวิทยาลัยแม่โจ้.

วรพจน์ วงศ์กิจรุ่งเรือง. (2561). คู่มือพลเมืองดิจิทัล. กรุงเทพฯ: สำนักงานส่งเสริมเศรษฐกิจดิจิทัล กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม.

โสภิตา วีรกุลเทวัญ. (2561). เท่าทันสื่อ อำนาจในมือพลเมืองดิจิทัล. กรุงเทพฯ : สถาบันสื่อเด็กและเยาวชน.

2. แนวทางการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัยและมีจริยธรรม

อัตราการเพิ่มของผู้ใช้งานอินเทอร์เน็ตทั่วโลกสูงขึ้นอย่างต่อเนื่อง และช่วงอายุของผู้ใช้งานกว้างมากขึ้นตั้งแต่ วัยเด็กจนถึงผู้สูงอายุ อินเทอร์เน็ตช่วยให้สามารถค้นหาข้อมูลที่ต้องการการติดต่อสื่อสารทำได้สะดวก แต่ในขณะเดียวกัน อินเทอร์เน็ตก็ได้สร้างปัญหาหลายประการให้กับผู้ใช้งาน เช่น ปัญหาทางด้านสุขภาพ เวลา และความเป็นส่วนตัว รวมถึงยังสร้างปัญหาที่นับว่าเป็นภัยสังคมอีกจำนวนไม่น้อย เช่น ปัญหาการล่อลวง ปัญหาการคุกคามทางเพศ ปัญหาการส่งข้อความหรือรูปภาพที่ผิดต่อหลักจริยธรรม ศีลธรรม และกฎหมาย ปัญหาการพนัน ปัญหาการวิจารณ์ และละเมิดสิทธิของผู้อื่น ปัญหาการขโมยข้อมูลสำคัญของส่วนบุคคล หรือองค์กร ดังนั้นการใช้อินเทอร์เน็ตจึงต้อง ตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับตนเองและผู้อื่น

การป้องกันปัญหาจากการใช้อินเทอร์เน็ตนั้นสามารถ ทำได้ โดยศึกษาหาความรู้เพื่อให้ใช้งานได้อย่างถูกต้อง ปฏิบัติ ตามข้อตกลงการใช้งาน เลือกสนทนาบนอินเทอร์เน็ตเฉพาะ ในกลุ่มที่ปลอดภัย หลีกเลี่ยง การนัดพบกับบุคคลที่รู้จักผ่านอินเทอร์เน็ต ในส่วนของผู้ให้บริการควรมีมาตรการเพื่อช่วย ป้องกันปัญหาที่อาจเกิดขึ้น เช่น ให้มีการลงทะเบียนสมาชิก ก่อนการใช้งาน มีระบบตรวจสอบและแจ้งเตือนรูปแบบ การสนทนาที่ไม่เหมาะสมอย่างสม่ำเสมอ

แนวทางปฏิบัติเมื่อพบเนื้อหาที่ไม่เหมาะสม ในการใช้อินเทอร์เน็ตนักเรียนจะพบข้อมูลที่หลากหลาย ทั้งข้อมูลที่ถูกต้องและข้อมูลที่มีการบิดเบือน หรือสร้างขึ้นเพื่อให้เกิดความเสียหายต่อผู้อื่นหรือส่วนรวม และหากนักเรียนพบข้อมูลที่ไม่เหมาะสมเหล่านั้น นักเรียนควรปฏิบัติดังนี้

1. ปฏิเสธการรับข้อมูล สามารถทำได้โดยไม่เปิดดู ไม่บันทึกเก็บไว้ และไม่กดไลค์ (Like) เพราะการกระทำเหล่านี้เป็นแนวทางที่ป้องกัน ไม่ให้ข้อมูลดังกล่าวเผยแพร่ไปสู่ผู้อื่น

2. ไม่ส่งต่อ ไม่แชร์ ไม่เผยแพร่ เพราะนอกจากจะทำให้ผู้อื่นเดือดร้อนกับข้อมูลที่ไม่เป็น ความจริงแล้ว ในบางกรณีอาจเข้าข่าย ผิดกฎหมายตามพระราชบัญญัติว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งมีโทษ ทั้งจำและปรับ

3. แจ้งครูหรือผู้ปกครอง หากนักเรียนประสบปัญหาที่ไม่สามารถจัดการหรือแก้ไขได้เอง ให้แจ้งครู หรือผู้ปกครองเพื่อดำเนินการแก้ไข หรือติดต่อประสานงานกับผู้เกี่ยวข้องเพื่อ ป้องกันไม่ให้เกิดปัญหาซ้ำเดิมไม่สิ้นสุด

4. แจ้งผู้เกี่ยวข้องที่ดูแลเว็บไซต์นั้น กรณีที่ใช้งานข้อมูลจากผู้ให้บริการระบบรายใหญ่ เช่น Facebook, YouTube ซึ่งเว็บไซต์เหล่านี้เปิดโอกาสให้ผู้ใช้งานสามารถรายงานปัญหา เกี่ยวกับเนื้อหาที่ไม่เหมาะสมได้ เช่น เนื้อหาที่มีการคุกคาม ทางเพศเนื้อหาเกี่ยวกับความรุนแรงส่งเสริมการก่อการร้าย การละเมิดลิขสิทธิ์หลังจาก ผู้ให้บริการได้รับแจ้ง จะมีการตรวจสอบเนื้อหา ดังกล่าวอย่างถี่ถ้วน และดำเนินการกับผู้กระทำผิด เช่น ลบเนื้อหา ตัดสิทธิ์ (Block) หรือจำกัดสิทธิ์การใช้งาน

5. แจ้งเจ้าหน้าที่รัฐหรือตำรวจ หากผู้ดูแลระบบไม่จัดการกับปัญหาที่เกิดขึ้น ให้ประสานงาน กับหน่วยงานรัฐที่มีหน้าที่รับผิดชอบโดยตรง เช่น แจ้งกระทรวงดิจิทัลเพื่อเศรษฐกิจและ สังคม ที่เว็บไซต์ <http://www.mdes.go.th> เพื่อดำเนินการตามกฎหมาย

ในสื่อสังคมออนไลน์จะพบว่ามีข้อมูลสารสนเทศที่หลากหลายที่เข้ามาให้เราพิจารณา การพิจารณา เนื้อหาก่อนการเผยแพร่ข้อมูล หรือการแชร์ข้อมูลนั้นก่อนที่นักเรียนจะเผยแพร่ข้อมูลใดลงในอินเทอร์เน็ต ควรพิจารณา ถึงจริยธรรมที่เกี่ยวข้องกับข้อมูลและการติดต่อสื่อสาร ซึ่งประกอบด้วย ความเป็นส่วนตัว (Privacy) ความถูกต้อง (Accuracy) ทรัพย์สิน (Property) และการเข้าถึง (Access) หรือเรียกย่อว่า พาปา (PAPA) ซึ่งมีรายละเอียดดังนี้

1) ความเป็นส่วนตัว (Information Privacy) หมายถึง สิทธิที่จะอยู่ตามลำพัง และเป็นสิทธิที่เจ้าของสามารถที่จะควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น สิทธินี้ใช้ได้ครอบคลุมทั้งปัจเจกบุคคล กลุ่มบุคคล และองค์การต่างๆ ปัจจุบันมีประเด็นเกี่ยวกับความเป็นส่วนตัวที่เป็นข้อน่าสังเกตดังนี้

1.1 การเข้าไปดูข้อความในจดหมายอิเล็กทรอนิกส์และการบันทึกข้อมูลในเครื่องคอมพิวเตอร์ รวมทั้งการบันทึก-แลกเปลี่ยนข้อมูลที่บุคคลเข้าไปใช้บริการเว็บไซต์และกลุ่มข่าวสาร

1.2 การใช้เทคโนโลยีในการติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคลซึ่งทำให้สูญเสียความเป็นส่วนตัว ซึ่งการกระทำเช่นนี้ถือเป็นการผิดจริยธรรม

1.3 การใช้ข้อมูลของลูกค้าจากแหล่งต่างๆ เพื่อผลประโยชน์ในการขยายตลาด

1.4 การรวบรวมหมายเลขโทรศัพท์ ที่อยู่อีเมล หมายเลขบัตรเครดิต และข้อมูลส่วนตัวอื่นๆ เพื่อนำไปสร้างฐานข้อมูลประวัติลูกค้าขึ้นมาใหม่ แล้วนำไปขายให้กับบุคคลอื่น

1.5 ดังนั้น เพื่อเป็นการป้องกันการละเมิดสิทธิความเป็นส่วนตัวของข้อมูลและสารสนเทศ จึงควรจะต้องระวังการให้ข้อมูล โดยเฉพาะการใช้อินเทอร์เน็ตที่มีการใช้โปรโมชัน หรือระบุให้มีการลงทะเบียนก่อนเข้าใช้บริการ เช่น ข้อมูลบัตรเครดิต หรือที่อยู่อีเมล

2) ความถูกต้อง (Information Accuracy) ในการจัดทำข้อมูลและสารสนเทศให้มีความถูกต้องและน่าเชื่อถือนั้น ข้อมูลควรได้รับการตรวจสอบความถูกต้องก่อนที่จะนำเข้าสู่ฐานข้อมูล รวมถึงการปรับปรุงข้อมูลใหม่ ความทันสมัยอยู่เสมอ นอกจากนี้ ควรให้สิทธิแก่บุคคลในการเข้าไปตรวจสอบความถูกต้องของข้อมูลตนเองด้วย

3) ความเป็นเจ้าของ (Information Property) สิทธิความเป็นเจ้าของ หมายถึง กรรมสิทธิ์ในการถือครองทรัพย์สิน ซึ่งอาจเป็นทรัพย์สินทั่วไปที่จับต้องได้ เช่น คอมพิวเตอร์ รถยนต์ หรืออาจเป็นทรัพย์สินทางปัญญา (ความคิด) ที่จับต้องไม่ได้ เช่น บทเพลงโปรแกรมคอมพิวเตอร์ แต่สามารถถ่ายทอดและบันทึกลงในสื่อต่าง ๆ ได้ เช่น สิ่งพิมพ์ เทป ซีดีรอม เป็นต้น โดยในการคัดลอกโปรแกรมคอมพิวเตอร์ให้กับเพื่อน เป็นการกระทำที่จะต้องพิจารณาให้รอบคอบก่อนว่าโปรแกรมที่จะทำการคัดลอกนั้น เป็นโปรแกรมคอมพิวเตอร์ที่ท่านมีสิทธิในระดับใด

4) การเข้าถึงข้อมูล (Data Accessibility) ปัจจุบันการเข้าใช้งานโปรแกรม หรือระบบคอมพิวเตอร์ มักจะมีการกำหนดสิทธิ์ตามระดับของผู้ใช้งาน ทั้งนี้ เพื่อเป็นการป้องกันการเข้าไปดำเนินการต่าง ๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้องและเป็นการอ้างไว้ซึ่งความลับของข้อมูล การเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอมนั้น ก็ถือเป็นการผิดจริยธรรมเช่นเดียวกับการละเมิดข้อมูลส่วนตัว

แนวทางการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัยและมีจริยธรรมเป็นสิ่งสำคัญจำเป็นในการใช้งานอินเทอร์เน็ตของผู้ใช้ เพื่อความปลอดภัยในข้อมูลของตนเองและไม่ไปละเมิดบุคคลอื่นในการใช้อินเทอร์เน็ต เพื่อให้นักเรียนเป็นพลเมืองดิจิทัลที่สมบูรณ์ ใช้อินเทอร์เน็ตอย่างปลอดภัยและรู้เท่าทัน

แหล่งที่มา

กิดานันท์ มลิทอง. (2543). เทคโนโลยีการศึกษาและนวัตกรรม. กรุงเทพมหานคร : ภาควิชาโสตทัศนศึกษาคณะครุศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี. (2562). เทคโนโลยี (วิทยาการคำนวณ). สำนักพิมพ์จุฬาลงกรณ์ : กรุงเทพมหานคร.

3. การรักษาข้อมูลส่วนตัวในโลกไซเบอร์

การปกป้องข้อมูลความส่วนตัวในโลกออนไลน์ของผู้ใช้งานที่บุคคลหรือหน่วยงานอื่นจะนำไปจัดเก็บนำไปใช้ประโยชน์ หรือนำข้อมูลนั้นไปเผยแพร่ ในปัจจุบัน ส่วนหนึ่งของข้อมูลส่วนตัวของเราได้ถูกจัดเก็บไว้โดยผู้ให้บริการโทรศัพท์ ผู้ให้บริการอินเทอร์เน็ต และผู้ให้บริการสื่อสังคมออนไลน์ ซึ่งมีนโยบายด้านความเป็นส่วนตัวของผู้ใช้งานในระดับหนึ่ง แต่ปัญหาอาจจะเกิดขึ้นได้หากข้อมูลส่วนตัวของเราตกไปอยู่ในมือของผู้ที่ไม่น่าไว้วางใจ ข้อมูลส่วนตัวของผู้ใช้งานอินเทอร์เน็ตอาจถูกละเมิดได้ เช่น บริษัทได้จัดเก็บและแบ่งปันข้อมูลส่วนตัวของผู้ใช้งานให้บริษัทอื่น ๆ การเจาะระบบความปลอดภัย (Hack) ของผู้ไม่หวังดีทำให้ข้อมูลส่วนตัวรั่วไหล การสอดแนมของรัฐบาล บริษัทสื่อกดรอยพฤติกรรมกรเข้าเว็บไซต์ของผู้ใช้งาน สื่อสังคมออนไลน์แบ่งปันข้อมูลส่วนตัวให้บุคคลอื่น หรือบริษัทอื่น ๆ

การรักษาข้อมูลส่วนตัวในอินเทอร์เน็ตจึงมีความสำคัญกับการดำเนินชีวิตในปัจจุบัน เนื่องจากเราไม่สามารถหลีกเลี่ยงการใช้ระบบต่าง ๆ บนอินเทอร์เน็ตได้ เช่น ระบบธนาคารอิเล็กทรอนิกส์ สื่อสังคมออนไลน์ในรูปแบบต่าง ๆ ทำให้เราจะต้องมีความสามารถในการป้องกันข้อมูลด้วยการป้องกันระบบความปลอดภัยที่เข้มแข็ง และป้องกันการโจรกรรมข้อมูลออนไลน์ได้ โดยทักษะในการรักษาความปลอดภัยของตนเองในโลกออนไลน์ คือการปกป้องอุปกรณ์ดิจิทัลข้อมูลที่จัดเก็บและข้อมูลส่วนตัวไม่ให้เสียหาย สูญหาย หรือถูกโจรกรรม อีกทั้งรักษาข้อมูลตนเองด้วยการป้องกันการเข้าถึงระบบต่าง ๆ ในอินเทอร์เน็ตจากผู้ไม่หวังดีในโลกไซเบอร์ การรักษาความปลอดภัยทางดิจิทัลมีความสำคัญดังนี้

1. การรักษาความเป็นส่วนตัวและความลับ หากไม่ได้รับการรักษาความปลอดภัยให้กับอุปกรณ์ดิจิทัล ข้อมูลส่วนตัวและข้อมูลที่เป็นความลับอาจจะรั่วไหลหรือถูกโจรกรรมได้

2. การป้องกันการขโมยอัตลักษณ์ การขโมยอัตลักษณ์เริ่มมีจำนวนที่มากขึ้นในยุคข้อมูลข่าวสาร เนื่องจากการทำธุรกรรมทางออนไลน์มากยิ่งขึ้น ผู้คนเริ่มทำการชำระค่าสินค้าผ่านสื่ออินเทอร์เน็ต และทำธุรกรรมกับธนาคารทางออนไลน์ หากไม่มีการรักษาความปลอดภัยที่เพียงพอ มีฉ้อโกงอาจจะล่วงล้ำข้อมูลเกี่ยวกับบัตรเครดิตและข้อมูลส่วนตัวของผู้ใช้งานไปสวมรอยทำธุรกรรมได้ เช่น ไปซื้อสินค้า กู้ยืมเงินหรือสวมรอยรับผลประโยชน์และสวัสดิการ

3. การป้องกันการโจรกรรมข้อมูล เนื่องจากข้อมูลต่าง ๆ มักเก็บรักษาในรูปของดิจิทัล ไม่ว่าจะเป็นเป็นเอกสารภาพถ่าย หรือคลิปวิดีโอ ข้อมูลเหล่านี้อาจจะถูกโจรกรรมเพื่อนำไปขายต่อ แบล็กเมล์ หรือเรียกค่าไถ่

4. เพื่อป้องกันความเสียหายของข้อมูลและอุปกรณ์ ภัยคุกคามทางไซเบอร์อาจส่งผลเสียต่อข้อมูลและอุปกรณ์ดิจิทัลได้ ผู้ไม่หวังดีบางรายอาจมุ่งหวังให้เกิดอันตรายต่อข้อมูลและอุปกรณ์ที่เก็บรักษามากกว่าที่จะโจรกรรมข้อมูลนั้น ภัยคุกคามอย่างไวรัสคอมพิวเตอร์ โทรจัน และมัลแวร์สร้างความเสียหายร้ายแรงให้กับคอมพิวเตอร์หรือระบบปฏิบัติการได้

แนวคิดหนึ่งที่ใช้สำหรับการป้องกัน ภัยคุกคามด้านไอที คือการตรวจสอบ และ ยืนยันตัวตนของผู้ใช้งานก่อนการเริ่มต้น ใช้งาน การตรวจสอบเพื่อยืนยันตัวตน ของผู้ใช้งานสามารถดำเนินการได้ 3 รูปแบบดังนี้

1. ตรวจสอบจากสิ่งที่ผู้ใช้รู้

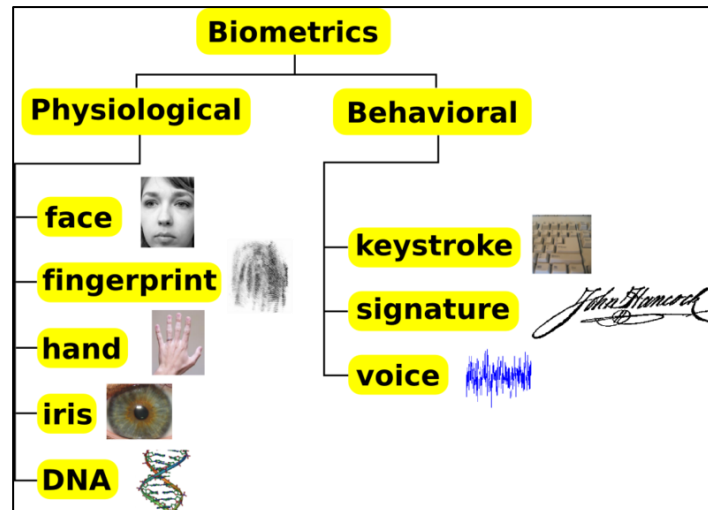
เป็นการตรวจสอบตัวตนจากสิ่งที่ผู้ใช้งานรู้ แต่เพียงผู้เดียว เช่น บัญชีรายชื่อผู้ใช้กับรหัสผ่าน การตรวจสอบวิธีนี้เป็นวิธีที่ได้รับความนิยมสูงสุด เนื่องจากเป็นวิธีที่ง่าย และระดับของความปลอดภัย เป็นที่ยอมรับได้ หากนักเรียนลืมหรหัสผ่าน สามารถติดต่อผู้ดูแลเพื่อขอรหัสผ่านใหม่

2. ตรวจสอบจากสิ่งที่ผู้ใช้มี

เป็นการตรวจสอบตัวตนจากอุปกรณ์ที่ผู้ใช้งาน ต้องมี เช่น บัตรสมาร์ทการ์ด อย่างไรก็ตาม การตรวจสอบวิธีนี้มีค่าใช้จ่ายในส่วนของอุปกรณ์ เพิ่มเติม และมักมีปัญหา คือ ผู้ใช้งานมักลืมหรือทำ อุปกรณ์ที่ใช้ตรวจสอบหาย

3. ตรวจสอบจากสิ่งที่เป็นส่วนหนึ่งของผู้ใช้

เป็นการตรวจสอบข้อมูลชีวมาตร (Biometrics) เช่น ลายนิ้วมือ ม่านตา ใบหน้า เสียง การตรวจสอบนี้ที่มีประสิทธิภาพสูงสุด แต่มีค่าใช้จ่ายที่สูงเมื่อเปรียบ เทียบกับวิธีอื่น และต้องมีการจัดเก็บลักษณะเฉพาะ ของบุคคล ซึ่งผู้ใช้บางส่วนอาจจะเห็นว่าเป็นการ ละเมิดสิทธิความเป็นส่วนตัว



ภาพตัวอย่างรูปแบบการตรวจสอบข้อมูลชีวมาตร (Biometrics)

ที่มา https://th.m.wikipedia.org/wiki/ไฟล์:Biometrics_traits_classification.png , Alessio Damato

สื่อสังคมออนไลน์มีระบบการตั้งค่าความเป็นส่วนตัวให้ผู้ใช้ปรับเปลี่ยนให้เข้ากับตัวผู้ใช้งาน ข้อมูลที่สื่อสังคมออนไลน์จัดเก็บมี 2 ประเภทคือ

1. ข้อมูลที่ผู้ใช้งานแชร์ลงสื่อออนไลน์ สื่อสังคมออนไลน์ไม่จัดเก็บข้อมูลของผู้ใช้งานไว้ในคอมพิวเตอร์ของผู้ใช้ แต่เก็บไว้ในที่เก็บข้อมูลของผู้ให้บริการแทน ข้อมูลเหล่านี้ได้แก่ รูปภาพและคลิปวิดีโอ อายุและเพศประวัติส่วนตัว เช่น โรงเรียน ที่ทำงาน บ้านเกิด การอัปเดตสถานภาพ รายชื่อผู้ติดต่อ ความสนใจ สถานที่อยู่ ข้อมูลเหล่านี้จะเปิดเผยต่อสาธารณะ ในกรณี ผู้ใช้งานเลือกที่จะโพสต์ข้อมูลเหล่านี้ในโหมด “สาธารณะ” บางข้อมูลจะเปิดเผยสู่สาธารณะตามการตั้งค่าเริ่มต้น ของผู้ให้บริการสื่อสังคมออนไลน์นั้น บางกรณีผู้ใช้งานสามารถตั้งค่าความเป็นส่วนตัวใหม่ได้ โดยจำกัดว่าใครเข้าถึงข้อมูลได้ ผู้ติดต่อคนอื่นของผู้ใช้งานที่ได้รับอนุญาตสามารถบันทึกและแบ่งปันข้อมูล เช่น รูปภาพของผู้ใช้งานได้โดยไม่ต้องได้รับอนุญาตจากผู้ใช้งาน แอปพลิเคชันภายนอก (Third-party applications) ที่ได้รับอนุญาตจากผู้ใช้งานสามารถเข้าถึงข้อมูลที่ผู้ใช้งานโพสต์ในโหมดความเป็นส่วนตัวได้ อย่างไรก็ตาม ผู้ให้บริการสื่อสังคมออนไลน์ไม่อาจรับประกันความปลอดภัยของข้อมูลส่วนตัวของผู้ใช้งานได้ แม้ว่าผู้ใช้งานจะตั้งค่าความเป็นส่วนตัวไว้แล้วก็ตาม เนื่องจากภัยคุกคามในโลกออนไลน์มีหลายรูปแบบ

2. ข้อมูลที่จัดเก็บผ่านระบบการสะกดรอยทางอิเล็กทรอนิกส์ (Electronic Tracking) ข้อมูลความเคลื่อนไหวออนไลน์ของผู้ใช้จะถูกจัดเก็บไว้ในระบบคุกกี้ ซึ่งจะสะกดรอยผู้ใช้งานจากเว็บหนึ่งไปสู่อีกเว็บหนึ่ง

โดยหากเป็นข้อมูลที่อยู่ในระบบต่าง ๆ บนอินเทอร์เน็ต หรือสื่อสังคมออนไลน์ขอแนะนำในการตั้งและใช้งานรหัสผ่าน โดยการกำหนดรหัสผ่านเป็นวิธีการตรวจสอบตัวตนที่นิยมมากที่สุด เนื่องจากว่าเป็นวิธีที่ง่ายและค่าใช้จ่ายน้อยกว่าเมื่อเทียบกับวิธีอื่น สิ่งที่ต้องคำนึงถึงในการกำหนดรหัสผ่านให้มีความปลอดภัยมีดังนี้

1. รหัสผ่านควรตั้งให้เป็นไปตามเงื่อนไข ของระบบที่ใช้งาน รหัสผ่านที่ดีควร ประกอบด้วย อักษรตัวใหญ่ ตัวเล็กตัวเลข และสัญลักษณ์ เช่น YinG@##lz หรือ @uG25SX*

2. หลีกเลี่ยงการตั้งรหัสผ่านโดยใช้วัน เดือน ปีเกิด ชื่อผู้ใช้ ชื่อจังหวัด ชื่อตัวละคร ชื่อสิ่ง ของต่าง ๆ ที่เกี่ยวข้อง หรือคำที่มีอยู่ใน พจนานุกรม

3. ตั้งให้จดจำได้ง่าย แต่ยากต่อการคาดเดา ด้วยบุคคลหรือโปรแกรม เช่น สร้างความสัมพันธ์ของรหัสผ่านกับข้อความหรือข้อมูล ส่วนตัวที่คุ้นเคย เช่น ตั้งชื่อสุนัขตัวแรก แต่เขียนตัวอักษรจากหลังมาหน้า

4. บัญชีรายชื่อผู้ใช้แต่ละระบบ ควรใช้รหัสผ่าน ที่แตกต่างกัน โดยเฉพาะบัญชีที่ใช้เข้าถึงข้อมูลที่มีความสำคัญ เช่น รหัสผ่านของบัตร เอทีเอ็มหลายใบให้ใช้รหัสผ่านต่างกัน

5. ไม่บันทึกหรือพิมพ์รหัสผ่านแบบอัตโนมัติบนโปรแกรม เบราวเซอร์ โดยเฉพาะอย่างยิ่งหากใช้เครื่องคอมพิวเตอร์ร่วมกับผู้อื่น หรือเครื่องสาธารณะ

6. ไม่บอกหรือพิมพ์รหัสผ่านของตนเองให้กับผู้อื่น ไม่ว่ากรณีใด ๆ

7. หมั่นเปลี่ยนรหัสผ่านเป็นประจำ อาจกระทำ ทุก 3 เดือน

8. หลีกเลี่ยงการบันทึกหรือพิมพ์รหัสผ่านลงในกระดาษ สมุดโน้ต รวมทั้งอุปกรณ์อิเล็กทรอนิกส์ด้วย หากจำเป็นต้องบันทึกก็ควรจัดเก็บไว้ในที่ ปลอดภัย

9. ออกจากระบบทุกครั้งเมื่อเลิกใช้บริการต่าง ๆ บนอินเทอร์เน็ต

การรักษาข้อมูลส่วนตัวในโลกไซเบอร์จึงเป็นสิ่งสำคัญในการดำเนินชีวิตประจำวัน บุคคลจะต้องมีความสามารถและทักษะในการรักษาข้อมูลส่วนตัวของตนเองบนอินเทอร์เน็ตจากระบบต่าง ๆ ไม่ว่าจะเป็นระบบธนาคารอิเล็กทรอนิกส์ ระบบบัตรเครดิต หรือแม้แต่สื่อสังคมออนไลน์ จะทำให้บุคคลมีความปลอดภัยจากการถูกละเมิดข้อมูลส่วนตัวของผู้ใช้งานได้

แหล่งที่มา

สถาบันสื่อเด็กและเยาวชน. (5 เมษายน 2563). การพัฒนาพลเมือง MILD จุดเน้นตามช่วงวัย,สืบค้นเมื่อ 5 เมษายน 2563, จาก <http://cclickthailand.com/ชุดความรู้สำหรับครู/ความรู้/การพัฒนาพลเมือง-midl-จุดเน้นตามช่วงวัย>.

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี. (2562). เทคโนโลยี (วิทยาการคำนวณ). สำนักพิมพ์จุฬาลงกรณ์ : กรุงเทพมหานคร.

4. การรับมือการคุกคามทางออนไลน์

ปัญหาเด็กและเยาวชนถูกลั่นแกล้งในสถานศึกษานั้น เป็นปัญหาที่เกิดขึ้นมานานแล้วในสังคมไทย แต่ปัจจุบันพฤติกรรมการกลั่นแกล้งในสังคมของเด็กและเยาวชนได้มีรูปแบบที่เปลี่ยนไป เนื่องจากวิวัฒนาการทางการสื่อสารของมนุษย์ได้พัฒนาเข้าสู่ยุคของสังคมออนไลน์การกลั่นแกล้งทางกายภายในอดีตจึงเปลี่ยนเป็นการคุกคามออนไลน์ (Cyber Bullying) โดยใช้เทคโนโลยีสารสนเทศและการสื่อสารต่าง ๆ เช่น จดหมายอิเล็กทรอนิกส์ (E-mail), โทรศัพท์เคลื่อนที่ (Cell phone), ระบบส่งข้อความทันที (Instant messaging) หรือสังคมออนไลน์ (Social Networking) เป็นเครื่องมือในการสนับสนุนพฤติกรรมการกลั่นแกล้งแทนการใช้กำลัง เทคโนโลยีสารสนเทศและการสื่อสารที่เข้าถึงได้ง่ายและสามารถเผยแพร่ในวงกว้างในระยะเวลาอันรวดเร็ว ส่งผลให้พฤติกรรมการกลั่นแกล้งของเด็กและเยาวชนขยายขอบเขตออกไปนอกสถานศึกษาเด็กและเยาวชนจึงอาจเผชิญกับการถูกลั่นแกล้งออนไลน์ได้ในทุกเวลาและทุกสถานที่แม้แต่ในบริเวณเคหสถานส่วนบุคคล

การรับมือการคุกคามทางออนไลน์เป็นพฤติกรรมในการรังแกหรือคุกคามผู้อื่น ซ้ำ ๆ โดยมีเจตนาในการสร้างความเจ็บปวดให้ผู้อื่นได้รับผลกระทบทางจิตใจ ผ่านช่องทางออนไลน์ หรืออุปกรณ์อิเล็กทรอนิกส์อื่น ๆ โดยที่ไม่ได้จำกัดรูปแบบพฤติกรรมหรืออุปกรณ์ที่ใช้ โดยผู้รังแกจะเปิดเผย หรือปิดบังตัวตนก็ได้ เช่น การโจมตีหรือใช้วาจาหยาบคายถูกเหยียดหยาม การคุกคามข่มขู่ การคุกคามทางเพศออนไลน์ การใส่ความ การแอบอ้างตัวตนของผู้อื่น การขโมยอัตลักษณ์ดิจิทัล การเผยแพร่ความลับ การหลอกลวงในรูปแบบต่าง ๆ การสร้างบัญชีปลอมเพื่อโจมตีบุคคลที่ตัวเองไม่ชอบ การกีดกันผู้อื่นออกจากกลุ่ม

โดย ญัฐรัชต์ สาเมาะ (2556) ได้ศึกษาการแบ่งรูปแบบของการรังแกกันผ่านโลกไซเบอร์ไว้ ดังนี้

1. การโจมตีด่าทอกันผ่านอินเทอร์เน็ตและโทรศัพท์มือถือ ได้แก่ การด่าทอ หรือพูดจาส่อเสียด การนิทาผ่านเครือข่ายสังคมออนไลน์ หรือมีสายโทรศัพท์โทรมาด่าเพื่อความสะใจ
2. การคุกคามทางเพศออนไลน์ ได้แก่ การพูด หรือบีบบังคับให้มีการแสดงกิจกรรมทางเพศผ่านกล้อง หรือเว็บแคม และส่งรูปภาพหรือวิดีโอในลักษณะโป๊ เปลือย โดยที่ผู้รับไม่ต้องการ
3. การแอบอ้างตัวตนของผู้อื่น ได้แก่ การขโมยรหัสผ่านบัญชีของผู้อื่นมาใช้แอบอ้างชื่อของผู้อื่นเพื่อให้ร้าย ด่าทอ หรือกระทำการประสังค์ร้าย รวมถึงสวมรอยในเครือข่ายสังคมของผู้อื่นเพื่อสร้างความเสียหายในรูปแบบต่าง ๆ
4. การแบล็กเมลกัน ได้แก่ การนำข้อมูลส่วนตัวความลับของผู้อื่นในรูปแบบข้อความภาพหรือวิดีโอไปเผยแพร่ การใส่ร้ายป้ายสีผู้อื่น เช่น การนำภาพเพื่อนแบบหลุด ๆ ไปแสดงความคิดเห็นอย่างสนุกสนานหรือตัดต่อรูปภาพแล้วใส่ข้อความที่ก่อให้เกิดความเสียหาย

5. การหลอกลวงออนไลน์ ได้แก่ การโฆษณาหลอกลวงให้หลงเชื่อ เพื่อจำหน่ายสินค้าลอกเลียนแบบ หลอกลวงให้มีการโอนเงินในลักษณะต่าง ๆ รวมถึงการหลอกลวงด้วยการนัดเจอกันในขณะที่อีกฝ่ายไม่ยินยอม

6. การสร้างกลุ่มเพื่อโจมตีบุคคลที่ตัวเองไม่ชอบ ได้แก่ การสร้างกลุ่มในเครือข่ายสังคมออนไลน์เพื่อโจมตีเพื่อนที่ตนเองไม่ชอบ หรือบุคคลที่มีชื่อเสียงที่ตนไม่ชอบอย่าง เช่น ดารา นักแสดง หรือนักการเมือง เป็นต้น

ในแง่ของผลกระทบจากการรังแกกันผ่านโลกไซเบอร์ ส่งผลกระทบต่อจิตใจของผู้ที่ถูกคุกคามมากกว่าการรังแกในพื้นที่จริง เนื่องจากพื้นที่บนโลกไซเบอร์จะแพร่กระจายในวงกว้าง จึงทำให้มีผู้คนรับรู้ถึงเหตุการณ์ดังกล่าวเป็นจำนวนมาก อีกทั้งข้อมูลที่กระจายออกไปจะยังคงค้างอยู่ในโลกไซเบอร์ไปตลอด ผลกระทบจากการรังแกกันผ่านโลกไซเบอร์จึงส่งผล ทั้งด้านของอารมณ์ ความรู้สึก และจิตใจ เนื่องจากการถูกรังแกจะทำให้เยาวชนรู้สึกแค้น รำคาญ และเสียใจ จนนำไปสู่ผลกระทบในมิติสุขภาพก่อให้เกิดความเครียด วิตกกังวล หดหู่ และไม่สบายใจ ซึ่งความรู้สึกเหล่านี้จะส่งผลกระทบต่อสุขภาพในระยะยาว ทำให้อนอนไม่หลับ คิดมาก และในกรณีที่

ร้ายแรงมาก ๆ อาจนำไปสู่การฆ่าตัวตายได้ในที่สุด ซึ่งการรังแกกันไม่ว่าจะเป็นโลกทางกายภาพ หรือโลกไซเบอร์มีผลกระทบที่ร้ายแรง โดยบางครั้งถึงขั้นเสียชีวิตจากการฆ่าตัวตาย เนื่องจาก ผู้ถูกรังแกจะเกิดความเครียดจากการถูกรังแก ซึ่งจากข่าวสารในต่างประเทศมีให้เห็นหลายกรณี เช่น ในประเทศญี่ปุ่น นักเรียนอายุ 18 ปี ตัดสินใจกระโดดตึกฆ่าตัวตายในโรงเรียน หลังจากที่เพื่อนร่วมชั้นนำภาพเปลือยไปเผยแพร่ผ่านเว็บไซต์พร้อมข่มขู่เรียกเงินจำนวนหนึ่ง หรืออีกกรณีหนึ่ง นักเรียนอเมริกันอายุ 15 ปี ฆ่าตัวตายเพราะถูกนักเรียนหญิงรุ่นพี่คุกคามผ่านข้อความสั้น และผ่านเฟซบุ๊กเพราะไม่พอใจเรื่องชู้สาว เป็นต้น และด้านการมีปฏิสัมพันธ์ทางสังคม ส่งผลให้ผู้ถูกรังแกรู้สึกอับอาย ทำให้คนในสังคมเข้าใจตัวเองผิด และดูไม่ดีในสายตาของคนอื่น ในบางกรณีจะทำให้รู้สึกอับอายจนไม่กล้าออกไปพบเจอผู้คน

ปัจจัยที่สำคัญที่สุดที่จะช่วยป้องกันปัญหาการคุกคามทางออนไลน์ของวัยรุ่นได้นั้น คือ ตัวของวัยรุ่นเอง วัยรุ่นควรที่จะมีการเรียนรู้มารยาทของการใช้การสื่อสารผ่านทางพื้นที่ไซเบอร์ต่าง ๆ ไม่ว่าจะเป็น Facebook, Twitter, Line, Youtube, E-mail หรือ พื้นที่ออนไลน์อื่น ๆ เพื่อป้องกันปัญหาและผลกระทบที่อาจเกิดขึ้นกับทั้งตัวผู้กระทำเองหรือผู้ถูกกระทำเองหลังการลงรูป วิดีโอ หรือข้อความที่อาจไม่เหมาะสมทั้งที่ตั้งใจและไม่ตั้งใจก็ตาม โดยวัยรุ่นควรปฏิบัติดังนี้

1. สร้างความตระหนัก

วัยรุ่นต้องตระหนักถึงมารยาทในการสื่อสารกับบุคคลอื่นถึงแม้ว่าจะเป็นการสื่อสารผ่านกลุ่มที่เป็นกลุ่มเฉพาะบุคคล พึงตระหนักเสมอว่าจงปฏิบัติต่อบุคคลอื่นให้เหมือนกับที่เราอยากให้คนอื่นปฏิบัติกับเราทั้งการสื่อสารในโลกของความเป็นจริงและการสื่อสารผ่านโลกไซเบอร์

2. คิดก่อนโพสต์

ไม่ว่าจะโพสต์ข้อความใด ๆ ก็ตาม เช่น รูปภาพ วิดีโอ หรือข้อความต่าง ๆ ให้คิดถึงผลกระทบทั้งผลดีและผลเสียที่อาจจะเกิดขึ้นตามมามาก่อนทุกครั้ง เพราะเมื่อโพสต์ลงไปในพื้นที่ไซเบอร์แล้ว ข้อความ รูปภาพ หรือวิดีโอดังกล่าวอาจย้อนกลับมาทำร้ายทั้งตัวผู้โพสต์เองและผู้ที่ถูกโพสต์ถึงซ้ำแล้วซ้ำอีกจนอาจก่อให้เกิดบาดแผลลึกทางจิตใจของทั้งตัวผู้โพสต์เองและผู้ที่ถูกโพสต์ถึงเอง แผลทางกายเมื่อเกิดขึ้นอาจจะง่ายที่จะรักษาให้เหมือนเดิม แต่แผลทางใจเมื่อเกิดขึ้นแล้วมันอยากนักที่จะรักษา และยิ่งถ้ามีผู้นำโพสต์ดังกล่าวที่เคยทำร้ายจิตใจผู้อื่นมาโพสต์ซ้ำก็ยิ่งเป็นการกริดร้อไปที่แผลทางใจของผู้นั้นอย่างไม่มีวันจบสิ้น

3. ให้ความสำคัญกับภาษาที่ใช้

การติดต่อสื่อสารกันผ่านสื่อสังคมออนไลน์นั้นทั้งผู้รับสารและผู้ส่งสารจะเห็นเพียงแต่ข้อความหรือรูปภาพที่ใช้ในการสื่อสารกัน แต่ขาดความเข้าใจถึงอารมณ์และความรู้สึกของผู้ส่งสารว่าในข้อความหนึ่ง ๆ ผู้ส่งสารต้องการสื่อสารให้ผู้รับสารทราบนั้น จริง ๆ แล้วผู้ส่งสารต้องการสื่อสารอะไร บ่อยครั้งที่เราต้องทะเลาะกันเพราะการสื่อสารผ่านทางสื่อสังคมออนไลน์ ดังนั้นก่อนที่จะโพสต์สิ่งใดก็ตาม หรือต้องการจะสื่อสารสิ่งใดก็ตามควรให้ความสำคัญถึงภาษาที่จะใช้ เพื่อป้องกันความเข้าใจผิดที่อาจเกิดขึ้นจากการสื่อสารที่ไม่สามารถเห็นหน้า หรือเห็นความรู้สึกของกันและกันได้

4. ข้อมูลส่วนตัวควรเป็นเรื่องส่วนตัว

การโพสต์ข้อมูลที่มีความเป็นส่วนตัวผิดที่ผิดเวลาสามารถนำมาซึ่งปัญหาที่ร้ายแรงต่อตัวผู้โพสต์เองได้ จะเห็นได้จากข่าวตามหน้าหนังสือพิมพ์หรือข่าวตามสังคมออนไลน์หลายครั้งที่การโพสต์ข้อมูลส่วนตัวของวัยรุ่นเองนำมาซึ่งปัญหาที่ร้ายแรงกับตัววัยรุ่น ไม่ว่าจะเป็นการถูกนำข้อมูลไปแอบอ้างในการกระทำความผิดต่าง ๆ เพราะฉะนั้นวัยรุ่นต้องพึงตระหนักไว้ว่าเมื่อไรก็ตามที่โพสต์ข้อมูลบางอย่างที่มีความเป็นส่วนตัวในสื่อสังคมออนไลน์ต่าง ๆ ไม่ว่าจะเป็น Facebook, Twitter, Line และอื่น ๆ เป็นการจำกัดความเป็นส่วนตัวของตัวเองวัยรุ่นเองมากขึ้นเท่านั้น

5. จำกัดเวลา

สิ่งสำคัญอีกอย่างหนึ่งที่วัยรุ่นควรทำ คือ การจำกัดเวลาในการใช้พื้นที่ไซเบอร์ หรือการสื่อสารผ่านสังคมออนไลน์ วัยรุ่นควรพยายามจำกัดเวลาหรือลดเวลาในการเล่นสื่อสังคมออนไลน์ และเพิ่มเวลาในการสื่อสารซึ่งกันและกันในโลกของความเป็นจริง เช่นการทำกิจกรรมกลางแจ้งต่าง ๆ ไม่ว่าจะเป็น การออกกำลังกาย หรือการไปทำกิจกรรมต่าง ๆ กับเพื่อนหรือครอบครัว แทนการใช้เวลาส่วนใหญ่ไปกับสังคมออนไลน์ โดยเฉพาะอย่างยิ่งเมื่อเกิดอารมณ์โกรธ หรือกำลังรู้สึกไม่พอใจกับสิ่งใดสิ่งหนึ่งหรือบุคคลใดบุคคลหนึ่ง วัยรุ่นไม่ควรระบายอารมณ์ของตนเองผ่านทางพื้นที่ไซเบอร์ในทันที แต่ควรหากิจกรรมอื่น ๆ ที่ไม่เกี่ยวข้องกับสื่อสังคมออนไลน์ทำ เพื่อช่วยเพิ่มเวลาในการคิดและไตร่ตรองก่อนที่จะโพสต์ข้อความ รูปภาพ วิดีโอ หรือข้อมูลอะไรต่าง ๆ ที่อาจย้อนกลับมาทำร้ายทั้งตนเองและคนอื่นได้ในภายหลัง

การจัดการเมื่อถูกกลั่นแกล้งบนโลกไซเบอร์เมื่อถูกกลั่นแกล้งบนโลกไซเบอร์ มีวิธีปฏิบัติง่าย ๆ ดังนี้

1. หยุด (Stop) หยุดการตอบโต้กับผู้กลั่นแกล้ง Logout จากบัญชีสื่อสังคมออนไลน์ หรือปิดเครื่องมือสื่อสาร
2. บล็อก (Block) ปิดกั้นการสื่อสารกับผู้กลั่นแกล้ง โดยการบล็อกจากรายชื่อผู้ติดต่อ
3. แจ้งให้ทราบ (Tell) ถ้าผู้กลั่นแกล้งยังไม่หยุดการกระทำอีก ควรรายงาน บอกผู้ปกครอง หรือครูที่ไว้วางใจรายงานไปยังผู้ให้บริการสื่อสังคมออนไลน์นั้นๆ ผู้กลั่นแกล้งอาจกระทำการละเมิดข้อตกลงการใช้งานสื่อออนไลน์ บันทึกหลักฐานการกลั่นแกล้ง อีเมล หรือภาพที่บันทึกจากหน้าจอ

แหล่งที่มา

ณัฐรัชต์ สาเมาะ. (2556). การรับรู้ของเยาวชนต่อการรังแกในพื้นที่ไซเบอร์. วิทยานิพนธ์ศิลปศาสตรมหาบัณฑิต. นครปฐม : มหาวิทยาลัยมหิดล.

สุวิพร ไฉสสถาพร. (2560). “ประสบการณ์และแนวทางการเผชิญปัญหาของเด็กและเยาวชนไทยที่ตกเป็นเหยื่อการกลั่นแกล้งทางไซเบอร์,” วิจัยและพัฒนาหลักสูตร. 7 (2), 215-234.

สถาบันสื่อเด็กและเยาวชน. (5 เมษายน 2563). การพัฒนาพลเมือง MILD จุดเน้นตามช่วงวัย,สืบค้นเมื่อ 5 เมษายน 2563, จาก <http://cclickthailand.com/ชุดความรู้สำหรับครู/ความรู้/การพัฒนาพลเมือง-midl-จุดเน้นตามช่วงวัย>.

5. ลิขสิทธิ์และความเป็นเจ้าของผลงาน

ปัจจุบันทรัพย์สินทางปัญญานับว่าเป็นสิ่งสำคัญยิ่ง และควรค่าต่อการที่จะได้รับความคุ้มครองตามกฎหมาย ด้วยเหตุผลที่ว่า การประดิษฐ์คิดค้น กรรมวิธีต่าง ๆ นั้น จุดกำเนิดของการได้มานั้นมาจากความคิดจากมันสมองผนวกกับระยะเวลาที่ทุ่มเทให้กับการศึกษาวิจัยเพื่อให้ได้มาซึ่งผลงานนวัตกรรมใหม่ ๆ ที่ทรงคุณค่าเป็นที่ภูมิใจของผู้ประดิษฐ์ ดังนั้นด้วยเหตุนี้เองผลงานดังกล่าวจึงควรค่าแก่การคุ้มครอง จากเหตุที่กล่าวมาจึงได้มีการบัญญัติเป็นกฎหมายเพื่อให้การคุ้มครอง โดยมีพระราชบัญญัติสิทธิบัตร ลิขสิทธิ์ เครื่องหมายการค้า ให้การคุ้มครองในหลักการรูปแบบที่แตกต่างกันไป

ลิขสิทธิ์ (Copyright) หมายถึง สิทธิแต่เพียงผู้เดียวของผู้สร้างสรรค์ที่จะกระทำการใด ๆ เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้นตามประเภทลิขสิทธิ์ที่กฎหมายกำหนด ได้แก่ งานวรรณกรรม นาฏกรรม ศิลปกรรม ดนตรีกรรม โสตทัศนวัสดุ ภาพยนตร์ สิ่งบันทึกเสียง งานแพร่เสียงแพร่ภาพ หรืองานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ ไม่ว่างานลักษณะดังกล่าวจะแสดงออกโดยวิธีหรือรูปแบบอย่างใด นอกจากนั้นกฎหมายลิขสิทธิ์ยังให้ความคุ้มครองถึงสิทธิของนักแสดงด้วย ลิขสิทธิ์เป็นทรัพย์สินทางปัญญาประเภทหนึ่ง ที่ผู้สร้างสรรค์ได้ริเริ่มโดยการใช้สติปัญญาความรู้ ความสามารถ และความวิริยะอุตสาหะของตนเอง ในการสร้างสรรค์โดยไม่ลอกเลียนงานของผู้อื่น โดยงานที่สร้างสรรค์ต้องเป็นงานตามประเภทที่กฎหมายลิขสิทธิ์คุ้มครอง โดยผู้สร้างสรรค์จะได้รับความคุ้มครองทันทีที่สร้างโดยไม่ต้องจดทะเบียน

สัญญาอนุญาตครีเอทีฟคอมมอนส์ (Creative Commons Licence: CC) เป็นสัญญาอนุญาตทางลิขสิทธิ์ประเภทหนึ่งพัฒนาโดย Hewlett Foundation study องค์กรไม่แสวงกำไรองค์กรหนึ่งที่เน้นงานด้านกฎหมาย ริชาร์ด สตอลแมน ได้สร้างตัวแปลชุดคำสั่งภาษา Lisp (ภาษาทางด้านโปรแกรม) โดยยกให้เป็นสาธารณะสมบัติ ต่อมาบริษัท Symbolics ได้พัฒนาภาษา Lisp ให้ดีขึ้นแต่ไม่ยอมเปิดเผยส่วนที่พัฒนาเพิ่มเติม แม้กระทั่งต่อ ริชาร์ด เอง จึงมีการสร้างสัญญาอนุญาตที่ชื่อว่า Copyleft (ไม่สงวนลิขสิทธิ์) ซึ่งตรงข้ามกับ Copyright (สงวนลิขสิทธิ์) ภายหลังจึงเกิดสัญญาอนุญาตซอฟต์แวร์เสรีชื่อว่า GNU General Public License (GPL) เพื่อปกป้องลิขสิทธิ์ซอฟต์แวร์แบบ Open Source ให้เจ้าของเผยแพร่ผลงานเป็นสาธารณะแต่ไม่เสียสิทธิในความเป็นเจ้าของ หลังจากนั้นได้มีการก่อตั้งองค์กรไม่แสวงกำไรที่ชื่อ “ครีเอทีฟคอมมอนส์” เพื่อสร้างสัญญาอนุญาตครีเอทีฟคอมมอนส์นี้

วัตถุประสงค์ของสัญญานี้เพื่อให้เจ้าของผลงานอันมีลิขสิทธิ์สามารถแสดงข้อความอันอำนวยความสะดวกให้สาธารณชนรู้ถึงสิทธิในผลงาน และทราบว่างานอันมีลิขสิทธิ์ของตนไปใช้ได้โดยไม่ต้องขออนุญาตและไม่ถือว่าเป็นการละเมิดลิขสิทธิ์ โดยผู้ที่นำผลงานไปใช้ต้องปฏิบัติตามเงื่อนไขที่กำหนดไว้ เช่น อ้างอิงแหล่งที่มา ไม่ใช่เพื่อการค้า ไม่ดัดแปลงต้นฉบับ เป็นต้น รายละเอียดของแต่ละสัญญานุญาตนั้น ขึ้นอยู่กับรุ่นของสัญญา และประกอบไปด้วยตัวเลือกจากเงื่อนไข 4 เงื่อนไข โดยได้มีการจัดทำสัญลักษณ์เงื่อนไขเป็น 4 ประเภท

ซึ่งเครือข่ายครีเอทีฟคอมมอนส์ประเทศไทย (<http://cc.in.th>) ได้ถอดความและนำสัญลักษณ์ 4 เงื่อนไขนั้นมาอธิบายไว้ดังนี้

1. แสดงที่มา/อ้างอิงที่มา (Attribution – BY) : อนุญาตให้ผู้อื่นทำซ้ำ แจกจ่าย หรือแสดงและนำเสนอชิ้นงานดังกล่าว และสร้างงานดัดแปลงจากชิ้นงานดังกล่าว ได้เฉพาะกรณีที่ผู้นั้นได้แสดงเครดิตของผู้เขียนหรือผู้ให้อนุญาตตามที่ระบุไว้ ใช้สัญลักษณ์



ภาพที่ 1 Attribution – BY

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

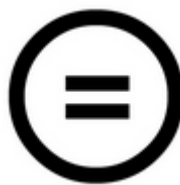
2. ไม่ใช่เพื่อการค้า (NonCommercial – NC) : อนุญาตให้ผู้อื่นทำซ้ำ แจกจ่าย หรือแสดงและนำเสนอชิ้นงานดังกล่าว และสร้างงานดัดแปลงจากชิ้นงานดังกล่าว ได้เฉพาะกรณีที่ไม่นำไปใช้ในทางการค้า ใช้สัญลักษณ์



ภาพที่ 2 NonCommercial – NC

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

3. ไม่ดัดแปลง (No Derivative Works – ND) : อนุญาตให้ผู้อื่นทำซ้ำ แจกจ่าย หรือแสดงและนำเสนอชิ้นงานดังกล่าวในรูปแบบที่ไม่ถูกดัดแปลงเท่านั้น ใช้สัญลักษณ์



ภาพที่ 3 No Derivative Works – ND

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

4. อนุญาตแบบเดียวกัน (Share Alike – SA) : อนุญาตให้ผู้อื่นแจกจ่ายงานดัดแปลง เปลี่ยนรูปหรือต่อเติมงานได้เฉพาะกรณีที่ชิ้นงานดัดแปลงนั้นเผยแพร่ด้วยสัญญาอนุญาตที่เหมือนกันทุกประการกับงานต้นฉบับ หรือสรุปง่ายๆ ว่าต้องใช้สัญญาอนุญาตชนิดเดียวกันกับงานดัดแปลงต่อยอดใช้สัญลักษณ์



ภาพที่ 4 Share Alike – SA

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

ทั้งนี้การกำหนดสัญญาอนุญาต ทำได้โดยการระบุเงื่อนไขร่วมกันได้ใน 6 แบบ ดังนี้

1. Attribution CC – BY ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มา สัญญาอนุญาตประเภทนี้อนุญาตให้ผู้อื่นดัดแปลง และต่อยอดงานของคุณ ถึงแม้ว่าจะนำไปใช้เพื่อการค้า トラバドイトที่คนที่น่าสนใจผลงานคุณไปใช้ให้เครดิต/อ้างอิงคุณในฐานะผู้สร้างงานต้นฉบับ



ภาพที่ 5 Attribution CC – BY

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

2. Attribution CC – BY -SA ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มาและต้องเผยแพร่งานดัดแปลงโดยใช้สัญญาอนุญาตเดียวกัน สัญญาอนุญาตรูปแบบนี้อนุญาตให้ผู้อื่นดัดแปลง แก้ไข หรือต่อยอดผลงานของคุณ หรือนำไปใช้เพื่อการค้า トラバドイトที่ผู้ใช้ให้เครดิต อ้างอิงคุณในฐานะของผู้สร้างผลงาน และลิงก์กลับมายังคุณ และใช้สัญญาอนุญาตแบบเดียวกันแบบเดียวกับคุณที่เป็นผู้สร้างงาน



ภาพที่ 6 Attribution CC – BY -SA

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

3. Attribution CC – BY -ND ให้เผยแพร่ โดยต้องระบุที่มา แต่ห้ามดัดแปลง สัญญาอนุญาตรูปแบบนี้อนุญาตให้ผู้อื่นไปเผยแพร่ และสามารถนำไปใช้เพื่อการการค้าได้ トラバドイトที่ผู้ใช้ให้เครดิต อ้างอิงคุณในฐานะของผู้สร้างผลงาน และลิงก์กลับมายังคุณ และไม่ดัดแปลง ต่อเติม หรือแก้ไข ผลงานของคุณแต่อย่างใด



ภาพที่ 7 Attribution CC – BY -ND

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

4. Attribution CC- BY -NC ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มาแต่ ห้ามใช้เพื่อการค้า สัญญาอนุญาตรูปแบบนี้อุญาตให้ผู้อื่นดัดแปลงแก้ไข หรือต่อยอดผลงานของคุณ และไม่จำเป็นต้องใช้สัญญาอนุญาตแบบเดียวกับคุณ ตราบใดที่ผู้ใช้ให้เครดิต/อ้างอิงคุณในฐานะของผู้สร้างผลงาน และลิงก์กลับมายังคุณ และไม่ได้นำผลงานของคุณไปใช้เพื่อการค้า



ภาพที่ 8 Attribution CC- BY -NC

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

5. Attribution CC- BY – NC – SA ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มาแต่ห้ามใช้เพื่อการค้าและต้องเผยแพร่งานดัดแปลงโดยใช้สัญญาอนุญาตชนิดเดียวกัน สัญญาอนุญาตรูปแบบนี้อุญาตให้ผู้อื่นนำผลงานของคุณมาดัดแปลง แก้ไข หรือต่อยอดผลงานของคุณ ตราบใดที่ผู้ใช้ให้เครดิต อ้างอิงคุณในฐานะของผู้สร้างผลงาน และลิงก์กลับมายังคุณ และไม่ได้นำผลงานของคุณไปใช้เพื่อการค้า



ภาพที่ 9 Attribution CC- BY – NC – SA

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

6. Attribution CC- BY – NC -ND ให้เผยแพร่ โดยต้องระบุที่มาแต่ห้ามดัดแปลงและห้ามใช้เพื่อการการค้า สัญญาอนุญาตรูปแบบนี้นับได้ว่ามีข้อจำกัดสูงสุดในการใช้งาน เนื่องจากสัญญาอนุญาตรูปแบบนี้สามารถให้ผู้อื่นนำผลงานของคุณไปใช้ ตราบใดที่ผู้ใช้ให้เครดิต/อ้างอิงคุณในฐานะของผู้สร้างผลงาน และลิงก์กลับมายังคุณ แต่เขาไม่ได้รับสิทธิในการนำผลงานของคุณไปใช้เพื่อการค้า และดัดแปลง ต่อเติม หรือแก้ไขผลงานของคุณแต่อย่างใด



ภาพที่ 10 Attribution CC- BY – NC -ND

ที่มา, <https://creativecommons.org/about/downloads>, creativecommons

ตัวอย่างการใช้ สัญญาอนุญาตครีเอทีฟคอมมอนส์ (CC) เช่น กรณีที่มีหน่วยงานด้านการวิจัยแห่งหนึ่งได้เผยแพร่งานวิจัยบนเว็บไซต์และประกาศใช้สัญญาแบบ CC-BY-NC-SA กับผลงานที่เผยแพร่ ผู้ที่นำ ข้อมูลไปใช้ได้โดยไม่ต้องทำ หนังสือขออนุญาตหรือทำ สัญญาข้อตกลงกับหน่วยงานแห่งนี้ ปรากฏว่ามหาวิทยาลัยแห่งหนึ่งนำข้อมูลไปทำ วิจัยต่อยอดต้องเผยแพร่งานวิจัยนั้นสู่สาธารณะ แต่ถ้ามหาวิทยาลัยนั้นนำข้อมูลไปตีพิมพ์เป็นหนังสือแล้วจำหน่ายหน่วยงานแห่งนี้สามารถฟ้องร้องการละเมิดสัญญาได้ ดังนั้นผู้ใช้งานที่นำ เอาผลงานของผู้อื่นที่มีสัญลักษณ์ดังกล่าวโดยเฉพาะบนอินเทอร์เน็ตต้องปฏิบัติตามสัญญาดังกล่าวโดยเคร่งครัดด้วย ผู้ที่

ทำผิดเงื่อนไขในสัญญาอนุญาต เจ้าของผลงานสามารถฟ้องร้องและบังคับผู้ทำผิดเงื่อนไขได้ตามกฎหมาย ลิขสิทธิ์คุ้มครอง อ่านเพิ่มเติมกฎหมายลิขสิทธิ์

แหล่งที่มา

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี. (2562). เทคโนโลยี (วิทยาการคำนวณ). สำนักพิมพ์จุฬาลงกรณ์ : กรุงเทพมหานคร.

Creativecommons. (11 เมษายน 2563). สัญลักษณ์ Creativecommons. สืบค้นเมื่อ 11เมษายน 2563, จาก <https://creativecommons.org/about/downloads>

6. กฎหมายนำรู้เกี่ยวกับคอมพิวเตอร์และการกระทำความผิดทางคอมพิวเตอร์

พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีวัตถุประสงค์ในการปรับปรุงจุดอ่อนของกฎหมายว่าด้วยการกระทำความผิดเพื่อสร้างความสมดุลระหว่างสิทธิเสรีภาพและการเคารพสิทธิของบุคคลอื่น เพื่อให้มีความรอบคอบและคำนึงถึงทุกภาคส่วนที่มีส่วนได้ส่วนเสีย หรือได้รับผลกระทบจากการบังคับใช้กฎหมายฉบับนี้ จึงมีการดำเนินการปรับปรุงแก้ไขใน พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560

เหตุผลในการประกาศใช้ พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 คือ โดยที่ พรบ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการกระทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็วและโดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ดำเนินภารกิจในการกำหนดมาตรฐานและมาตรการในการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งการเฝ้าระวังและติดตามสถานการณ์ด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของประเทศ

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ฉบับแก้ไขล่าสุดคือฉบับที่ 2 มีผลบังคับใช้เมื่อวันที่ 24 พฤษภาคม 2560 ซึ่งตัว พรบ.คอมพิวเตอร์ นั้นได้กำหนดความผิดในการกระทำที่มีระบบคอมพิวเตอร์เข้ามาเกี่ยวข้อง ดังนั้นบุคคลผู้ใช้คอมพิวเตอร์หรือผู้ที่มีการใช้อินเทอร์เน็ตจำเป็นต้องทราบว่าข้อกำหนดนั้นมีอะไรบ้าง เพื่อป้องกันการทำความผิด พรบ. คอมพิวเตอร์ ซึ่งพรบ.คอมพิวเตอร์แก้ไขล่าสุด นี้ได้มีการแก้ไขทั้งหมด 21 มาตรา ในที่นี้จะกล่าวถึงข้อกำหนดในส่วนของคุณค่าของบุคคลทั่วไปควรระวังในการใช้คอมพิวเตอร์ ดังต่อไปนี้

1. การแฮ็กเฟซบุ๊ก (มาตรา 5-8)

การปลอมไอดี หรือมัลแวร์เข้าคอมพิวเตอร์คนอื่นเพื่อขโมยข้อมูล โดยที่เจ้าของไม่อนุญาต (ละเมิด Privacy) มีโทษฐานผิด พรบ.คอมพิวเตอร์

- เข้าถึงระบบคอมพิวเตอร์ จำคุกไม่เกิน 6 เดือน ปรับไม่เกิน 1 หมื่นบาท
- เข้าถึงข้อมูลคอมพิวเตอร์ จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท
- นำมาตรการป้องกันระบบไปเผยแพร่ จำคุกไม่เกิน 1 ปี ปรับไม่เกิน 2 หมื่นบาท
- ดักจับข้อมูลคอมพิวเตอร์ จำคุกไม่เกิน 2 ปี ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ!!

2. การแก้ไข ดัดแปลงข้อมูล (มาตรา 9-10)

การเข้าไปขัดขวาง ทำร้ายระบบ รวมทั้งเข้าไปดัดแปลง หรือทำลายข้อมูล ทำให้ข้อมูลของฝ่ายตรงข้ามเสียหายผิด พรบ.คอมพิวเตอร์ มีโทษจำคุก 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ

3. การฝากร้านใน Facebook และ IG ไม่สามารถทำได้ (มาตรา 11)

สำหรับบุคคลที่เป็นพ่อค้าแม่ขายบนโลกออนไลน์ เรื่องการส่งอีเมลขายของโดยที่ลูกค้าไม่ยินดียี่งที่จะรับนั้นถือเป็นการสแปม หรือแม้แต่การฝากร้านตาม Facebook และ Instagram ก็ตามมีโทษตาม พรบ.คอมพิวเตอร์ โดยปรับไม่เกิน 1 แสนบาท จำคุกไม่เกิน 2 ปี หรือทั้งจำทั้งปรับ

4. การเข้าระบบของหน่วยงานภาครัฐโดยไม่ได้รับอนุญาต (มาตรา 12)

การเข้าถึงระบบ หรือข้อมูลด้านความมั่นคงรวมถึงการโพสต์เนื้อหาที่ส่งผลกระทบต่อความมั่นคงต่อประเทศบนโลกออนไลน์ที่เข้าข่ายข้อมูลเท็จที่ทำให้ประชาชนเกิดอาการตื่นตระหนก มีโทษแบ่งตาม พรบ. คอมพิวเตอร์เป็นกรณีดังนี้

- กรณีไม่เกิดความเสียหาย จำคุก 1-7 ปี และปรับ 2 หมื่น – 1.4 แสนบาท
- กรณีเกิดความเสียหาย จำคุก 1-10 ปี และปรับ 2 – 2 แสนบาท
- กรณีเป็นเหตุให้ผู้อื่นถึงแก่ความตาย จำคุก 5 – 20 ปี และปรับ 1 แสน – 4 แสนบาท

5. การโพสต์ข่าวปลอม (มาตรา 14)

การโพสต์หรือจัดทำเนื้อหาว่าด้วยความผิด พรบ.คอมพิวเตอร์ เริ่มจากการโพสต์ ข่าวปลอม ธุรกิจลูกโซ่ ที่ต้องการจะหลอกเอาเงินจากลูกค้า โพสต์เกี่ยวกับความมั่นคงปลอดภัยรวมทั้งการก่อการร้าย โพสต์ข้อมูลลามก โดยถ้าเกิดว่าส่งผลถึงประชาชน จะต้องจำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสนบาท หรือทั้งจำทั้งปรับ ส่วนถ้าส่งผลกระทบต่อบุคคลใดบุคคลหนึ่ง จำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ

6. ความผิดในการแสดงความคิดเห็นในข่าวปลอม (มาตรา 15)

การที่บุคคลเข้าไปแสดงความคิดเห็นในโพสต์ที่มีเนื้อหาผิดกฎหมายก็จะกระทำความผิด พรบ.คอมพิวเตอร์ ถ้าไม่ยอมลบจะได้รับโทษเดียวกันกับมาตรา 14 เหมือนกันกับผู้โพสต์ แต่ถ้าหากว่าลบออกไปแล้ว ถือว่าพ้นผิด

7. การตัดต่อรูปภาพมีความผิด (มาตรา 16)

การตัดต่อ ดัดแปลงภาพที่ทำให้ผู้อื่นเสียชื่อเสียง และเกิดความเสียหาย รวมทั้งโพสต์ภาพผู้เสียชีวิตที่ทำให้พ่อ – แม่ คู่สมรส หรือบุตรของผู้ตายเสียชื่อเสียง ดูหมิ่นเกลียดชัง หรือได้รับความอับอาย จะต้องจำคุกไม่เกิน 3 ปี และปรับไม่เกิน 2 แสนบาท

8. กด Share ถือเป็นการเผยแพร่ หากข้อมูลที่แชร์มีผลกระทบต่อผู้อื่น อาจเข้าข่ายความผิดตาม พรบ.คอมพิวเตอร์ โดยเฉพาะที่กระทบต่อบุคคลที่ 3

9. พบข้อมูลผิดกฎหมายอยู่ในระบบคอมพิวเตอร์ของเรา แต่ไม่ใช่สิ่งที่เจ้าของคอมพิวเตอร์กระทำเอง สามารถแจ้งไปยังหน่วยงานที่รับผิดชอบได้ หากแจ้งแล้วลบข้อมูลออกเจ้าของก็จะเป็นความผิดตามกฎหมาย เช่น ความเห็นในเว็บไซต์ต่าง ๆ รวมไปถึงเฟซบุ๊ก ที่ให้แสดงความคิดเห็น หากพบว่าการแสดงความคิดเห็นผิดกฎหมาย เมื่อแจ้งไปที่หน่วยงานที่รับผิดชอบเพื่อลบได้ทันที เจ้าของระบบเว็บไซต์จะไม่มีผิด

10. สำหรับ แอดมินเพจ ที่เปิดให้มีการแสดงความคิดเห็น เมื่อพบข้อความที่ผิด พรบ.คอมพิวเตอร์ เมื่อลบออกจากพื้นที่ที่ตนดูแลแล้ว จะถือเป็นผู้พ้นผิด

11. การโพสต์เกี่ยวกับเด็ก เยาวชน ต้องปิดบังใบหน้า ยกเว้นเมื่อเป็นการเชิดชู ชื่นชม อย่างให้เกียรติ

ในการใช้คอมพิวเตอร์และสื่อสังคมออนไลน์บุคคลจะต้องมีความระมัดระวังในการโพสต์ข้อความ แชร์เนื้อหาต่าง ๆ ในระบบคอมพิวเตอร์ จะต้องมีการพิจารณาในการใช้สื่อสังคมออนไลน์ ไม่การโพสต์ข่าวปลอม ไม่การตัดต่อรูปภาพที่ทำให้ผู้อื่นได้รับความเสียหาย เป็นต้น

แหล่งที่มา

ปริญญา หอมเอนก. (10 เมษายน 2563). เปิดสาระสำคัญ กฎหมายคอมพิวเตอร์. สืบค้นเมื่อ 10 เมษายน 2563, จาก <https://www.bangkokbiznews.com/blog/detail/649170>.

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ.2560. สืบค้นเมื่อ 10 เมษายน 2563, จาก <http://www.ratchakitcha.soc.go.th/DATA/PDF/2560/A/010/24.PDF>.

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี. (2562). เทคโนโลยี (วิทยาการคำนวณ). สำนักพิมพ์จุฬาลงกรณ์ : กรุงเทพมหานคร.

สื่อ Infographic
รู้เท่าทันสื่อและเทคโนโลยีเพื่อป้องกันภัยไซเบอร์
สำหรับการดำเนินชีวิตวิถีใหม่และวิถีถัดไป



Malware หรือ Malicious Software

คือโปรแกรมคอมพิวเตอร์ทุกชนิด ที่ถูกออกแบบโดยมีวัตถุประสงค์ เพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย และก่อให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ เช่น ทำให้ระบบขัดข้องหรือเกิดความเสียหาย เป็นต้น



Virus

มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์ และสามารถแพร่กระจายไปยังเครื่องอื่น ๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น



ตัวอย่างไฟล์ที่มักพบไวรัสบ่อย เช่น Executable files (โปรแกรมต่าง ๆ บนคอมพิวเตอร์), Boot sectors (ส่วนของคำสั่งที่ไวติดต่อกับคอมพิวเตอร์เพื่อใช้ในการเรียกเปิดใช้งานระบบ), Scripting files (เช่น windows scripting หรือ visual basic script), Macro ในไฟล์เอกสาร เป็นต้น

Worm

สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่น ๆ ผ่านทางระบบเครือข่าย เช่น e-mail หรือระบบแชร์ไฟล์ โดยไม่ต้องอาศัยการเรียกใช้งานโปรแกรมจากผู้ใช้งาน



Bot



คือซอฟต์แวร์ที่สร้างขึ้นมาเพื่อทำงานใดงานหนึ่งแบบอัตโนมัติ โดยรับคำสั่งและควบคุมจากเครื่องของ hacker (command and control center) เช่น Botnets (เครื่องที่ถูก hacker ควบคุม) ใช้มาเพื่อการโจมตีแบบ DDoS หรือ Spambot เพื่อใช้สำหรับการส่ง Spam เป็นต้น โดยเครื่องที่ตกเป็นเหยื่อมักจะถูกเรียกว่า Drones หรือ Zombies

Trojan

เป็นโปรแกรมที่ระบุวัตถุประสงค์ให้ผู้ใช้ใช้งานเข้าใจว่าเป็นโปรแกรมสำหรับใช้งานตามที่กล่าวอ้างและปลอดภัย แต่แท้จริงแล้วได้แอบแฝงคำสั่งอันตราย (เช่น คำสั่งลบไฟล์ข้อมูล , เขียนทับข้อมูลใน hard-drive หรือ สร้างการเข้าถึงระยะไกล (remote access) บนเครื่องแม่ข่ายกลับไปยัง hacker เป็นต้น) ตัวอย่างเช่น Remote Access Tools (RATs หรือ Backdoors) , Keylogging และ password stealing (Spyware ส่วนใหญ่ก็จัดอยู่ในหมวดนี้)





Rootkit

เปิดช่องทางให้ผู้อื่นเข้ามาติดตั้งโปรแกรมเพิ่มเติม เพื่อควบคุมเครื่อง พร้อมได้สิทธิ์ของผู้ดูแลระบบ (Root)

Adware

เป็น malware ประเภทหนึ่งที่มาในรูปแบบโฆษณา หรือ บางครั้งก็เรียกเปิดหน้าเว็บเพื่อป๊อปอัพขึ้นมาโดยอัตโนมัติ



Spyware

เป็นโปรแกรมที่ใช้ในการติดตาม แอบดูพฤติกรรม และบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย และมักจะถูกติดตั้งโดยที่ผู้ใช้งาน ไม่ทันได้สังเกต หรือไม่มีการขอความยินยอมจากผู้ใช้งาน



Ransomware

คือ malware ที่มุ่งหวังจะทำการเข้ารหัสไฟล์ข้อมูลของเหยื่อเพื่อเรียกค่าไถ่ ซึ่งจะส่งผลให้เหยื่อหรือเจ้าของข้อมูลไม่สามารถเข้าถึงไฟล์ข้อมูลของตนเองได้ โดยเหยื่อจะต้องจ่ายเงินให้กับ hacker เพื่อทำการถอดรหัสไฟล์ข้อมูลดังกล่าว โดยไม่สามารถรับรองได้ว่า hacker จะทำการถอดรหัสไฟล์ให้เหยื่อหรือไม่ หลังได้รับค่าไถ่แล้ว ทั้งนี้ hacker มักจะให้ผู้เสียหายจ่ายค่าไถ่ผ่านสกุลเงินดิจิทัล เช่น Bitcoin เนื่องจากเป็นช่องทางที่ยากต่อการตรวจสอบ

Hoaxes



เป็นรูปแบบหนึ่งของการก่อวินาศกรรม โดยไวรัสหลอกลวงพวกนี้จะมาในรูปแบบของ e-mail การส่งข้อความต่อ ๆ กันไปผ่านทางโปรแกรมรับส่งข้อความ หรือห้องสนทนาซึ่งสามารถสร้างความวุ่นวาย โดยการใช้จิตวิทยาของผู้สร้างข่าวขึ้นมามีผลทำให้ผู้ได้รับข้อความเกิดความกลัว ความลังเล สงสัย และเมื่อผู้รับ ส่งต่อไปยังผู้อื่น ก็ยิ่งสร้างความเชื่อมั่นมากขึ้น จากนั้นผู้รับก็จะทำตัวเป็นผู้ส่งต่อไปอีกหลาย ๆทอด ซึ่งเป็นลักษณะเด่นของไวรัสนี้

Phishing



เทคนิคการหลอกลวงโดยใช้ e-mail หรือหน้าเว็บไซต์ปลอมเพื่อให้ได้มาซึ่งข้อมูลส่วนบุคคลต่าง ๆ เช่น ชื่อผู้ใช้อีเมล รหัสผ่าน วันเดือนปีเกิด เป็นต้น และใช้ข้อมูลดังกล่าวในการเข้าระบบโดยไม่ได้รับอนุญาต รวมถึงหลอกล่อให้เหยื่อกดลิงค์ เพื่อแอบติดตั้ง malware ลงคอมพิวเตอร์

โดยประเภทของ Phishing ที่พบเห็นโดยส่วนใหญ่ มี 2 ประเภทได้แก่ (1) **E-mail Phishing** และ (2) **Web Phishing** นอกจากนี้ยังมีเทคนิคการหลอกลวงอื่น ๆ ที่คล้ายคลึงกัน เช่น

Vishing โดยตัวอักษร 'V' นี้มาจากคำว่า Voice ซึ่งแปลว่าเสียง ดังนั้น Vishing จึงเป็นการใช้ Voice ร่วมกับ Phishing ซึ่งมักเป็นการหลอกลวงให้ได้มาซึ่งข้อมูลส่วนบุคคลผ่านทางโทรศัพท์นั่นเอง

Smishing เป็นการหลอกลวงโดยใช้ SMS เช่น การได้รับ SMS อ้างว่ามาจากธนาคารเพื่อแจ้งลูกค้าว่าบัญชีของท่านถูกระงับ กรุณาติดต่อกลับที่หมายเลขดังต่อไปนี้ ซึ่งเมื่อโทรตามหมายเลขที่ระบุไว้ ก็จะเข้าสู่กระบวนการ Vishing ต่อไป

ข้อแนะนำในการป้องกัน

1. อัปเดตคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ
2. ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์
3. ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย (Removable Media) เช่น External Harddisk Thumb Drive เป็นต้น โดยควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน
4. ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์โหลด malware จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ
5. ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เสี่ยงต่อการมี malware แฝงอยู่
6. หลีกเลี่ยงการเปิด e-mail รวมไปถึงไฟล์แนบที่ต้องสงสัยใด ๆ ที่ส่งมาจาก e-mail ที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา



สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์



www.sec.or.th



สำนักงาน ก.ล.ต.



1207

5 วิธีป้องกันภัยคุกคาม! ทางออนไลน์



1. ไม่เชื่อ ไม่บอก ไม่กรอกข้อมูลส่วนตัวที่สำคัญบนโลกออนไลน์
2. ไม่ดาวน์โหลดแอปหรือโปรแกรมที่น่าสงสัย
3. ไม่ใช้ wifi สาธารณะทำธุรกรรมเงิน
4. ตั้งรหัสผ่านให้คาดเดายาก และเปลี่ยนเป็นระยะ
5. ออกจากระบบทุกครั้งเมื่อเลิกใช้งาน

ที่มา : ศูนย์ประสานงานป้องกันภัยทางคอมพิวเตอร์ ธนาคารแห่งประเทศไทย

ANTI-FAKE NEWS CENTER ศูนย์ต่อต้านข่าวปลอม ประเทศไทย

Copyright © 2022, Anti-Fake News Center, All rights reserved



แหล่งเรียนรู้เพิ่มเติม

<https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-INFOG.aspx>

<https://www.sec.or.th/TH/Pages/CYBERRESILIENCE-KNOWLEDGECYBER.aspx>

https://www.sesapy.go.th/?page_id=6881

<https://learningdq-dc.ku.ac.th/course/?c=7&l=6>

<https://www.scimath.org/article-technology/item/11534-2020-05-01-03-32-41>

<https://www.antifakenewscenter.com/>