ใบความรู้ที่ 1.3 เรื่อง การใช้เทคโนโลยีสารสนเทศให้ปลอดภัย หน่วยที่ 1
แผนการจัดการเรียนรู้ที่ 1 เรื่อง เทคโนโลยีในชีวิตประจำวัน
รายวิชา เทคโนโลยี1 รหัส ว21103 ภาคเรียนที่ 2 ชั้นมัธยมศึกษาปีที่ 1

จุดประสงค์ อภิปรายวิธีการป้องกันและการแก้ปัญหาในการใช้เทคโนโลยีอย่างปลอดภัย

ปัจจุบันเทคโนโลยีสารสนเทศมีบทบาทต่อการดำรงชีวิตประจำวันของทุกเพศทุกวัย และทุกอาชีพ ทุกคนต้องปรับตัวในการใช้ชีวิตในแต่ละวัน เพื่อให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศในยุคที่สัญญาณอินเตอร์เน็ตครอบคลุมเกือบทุกพื้นที่ การใช้งานเทคโนโลยีสารสนเทศก็เปรียบเสมือนดาบสองคมที่มีทั้งผลดีและผลเสีย ผู้ใช้งานต้องรู้เท่าทันและสามารถใช้เทคโนโลยีสารสนเทศได้อย่างปลอดภัยมีจริยธรรมในการใช้เทคโนโลยีสารสนเทศ

1. ภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศและวิธีการป้องกัน

เทคโนโลยีสารสนเทศมีประโยชน์แต่ขณะเดียวกันก็ยังแฝงไว้ซึ่งภัยมาด้วยเช่นกัน การเชื่อมต่ออินเตอร์เน็ตช่วยให้สามารถติดต่อสื่อสารกันได้ทั่วโลกอย่างสะดวกและรวดเร็ว ถือว่าเป็นสังคมที่อยู่ร่วมกันเป็นมิติที่ซ้อนๆ กันย่อมมีทั้งคนดีและคนไม่ดีปะปนกันไป เราต้องใช้ความระมัดระวังมีจริยธรรมในการใช้งาน หากขาดความระมัดระวังอาจจะทำให้เกิดปัญหาจากการคุกคามหรืออาจถูกหลอกลวงได้ ดังนั้นการใช้งานเทคโนโลยีสารสนเทศจึงต้องใช้อย่างเหมาะสมและรู้จักวิธีการป้องกันตนเองด้วย

1.1 วิธีการคุกคามทางเทคโนโลยีสารสนเทศ

ภัยคุกคามมีหลายวิธีโดยมีตั้งแต่ใช้ความรู้ขั้นสูงด้านไอที ไปจนถึงวิธีวิธีที่ไม่จำเป็นต้องใช้ความรู้ทางด้านเทคนิค ดังนี้

1. การคุกคามโดยใช้หลักจิตวิทยา เป็นการคุกคามที่ใช้การหลอกลวงเพื่อให้ได้ข้อมูลที่ต้องการ เช่น การสร้างหน้าเว็บไซต์เลียนแบบเว็บไซต์ที่โด่งดัง เพื่อหลอกให้ผู้ใช้เข้าใจผิด แล้วหลงให้รหัสผ่าน การป้องกันคือผู้ใช้ต้องมีความระมัดระวังให้มั่นใจว่าเป็นเว็บไซต์ที่เชื่อถือได้หรือไม่ก่อนกรอกข้อมูลต่างๆ ลงไป

2. การคุกคามด้วยเนื้อหาที่ไม่เหมาะสม ข้อมูลและเนื้อหาที่มีอยู่ในแหล่งต่างๆ บนอินเตอร์เน็ตมีจำนวนมาก ทำให้ข้อมูลอาจจะไม่ได้รับการตรวจสอบ และในบางแหล่งข้อมูลอาจมีเนื้อหาไม่เหมาะสม ซึ่งการคุกคามแบบนี้ส่งผลเสียต่อวัยเด็กและวัยรุ่นเป็นอย่างมาก

3. การคุกคามโดยใช้โปรแกรม เป็นการคุกคามโดยการใช้เครื่องมือทางด้านไอที เพื่อก่อปัญหาให้กับผู้ใช้อื่นๆ ซึ่งเครื่องมือดังกล่าวเรียกว่า มัลแวร์ (Malicious Software: Malware) มีหลายประเภท เช่น

3.1 ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นโปรแกรมที่เขียนด้วยเจตนาร้าย อาจทำให้ผู้ใช้งานเกิดความรำคาญ หรือเกิดความเสียหายต่อระบบของผู้ใช้ ไวรัสคอมพิวเตอร์มักติดมากับไฟล์งานต่างๆ และจะทำงานเมื่อมีการเปิดไฟล์งานนั้นๆ

3.2 เวิร์ม (Worm) มีการเรียกเป็นภาษาไทยว่า “หนอนอินเตอร์เน็ต” เป็นโปรแกรมที่สามารถทำสำเนาตัวเอง (copy) และแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ ได้ ทำให้คอมพิวเตอร์และระบบเครือข่ายเสียหาย ต้องอัปเดตโปรแกรมที่ใช้ทั้งหมดให้ทันสมัยอยู่เสมอ หากคอมพิวเตอร์ทำงานช้าลง , คอมพิวเตอร์ไม่สามารถทำงานได้ และควรหลีกเลี่ยงการเปิดเมล์ที่เราไม่รู้จักหรือไม่แน่ใจ

3.3 ม้าโทรจัน (Trojan Horse Virus) คือโปรแกรมคอมพิวเตอร์ที่ถูกบรรจุเข้าไปในคอมพิวเตอร์ เพื่อลอบเก็บข้อมูลของคอมพิวเตอร์เครื่องนั้น เช่น ข้อมูลชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร ส่วนใหญ่แฮกเกอร์จะส่งโปรแกรมเข้าไปในคอมพิวเตอร์เพื่อดักจับข้อมูลดังกล่าว แล้วนำไปใช้ในการเจาะระบบและเพื่อโจมตีคอมพิวเตอร์

3.4 สปายแวร์ (Spyware) เป็นโปรแกรมเล็กๆ ที่ถูกเขียนขึ้นมาสอดส่อง (สปาย) การใช้งานเครื่องคอมพิวเตอร์ของผู้ใช้ อาจจะเพื่อโฆษณาสินค้าต่างๆ สปายแวร์บางตัวก็สร้างความรำคาญเพราะจะเปิดหน้าต่างโฆษณาบ่อยๆ แต่บางตัวทำให้ผู้ใช้ใช้อินเตอร์เน็ตไม่ได้เลย

3.5 โปรแกรมโฆษณา (Advertising Supported Software: Adware) คือโปรแกรมที่สามารถทำงาน แสดง หรือดาวน์โหลดสื่อโฆษณาโดยอัตโนมัติ ไปยังคอมพิวเตอร์ที่ได้รับการติดตั้งโปรแกรมชนิดนี้ไว้

3.6 โปรแกรมเรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ประเภทหนึ่งที่มีลักษณะการทำงานที่แตกต่างกับมัลแวร์ประเภทอื่นๆ คือไม่ได้ถูกออกแบบมาเพื่อขโมยข้อมูลของผู้ใช้ แต่จะทำการเข้ารหัสหรือล็อคไฟล์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใดๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ

3.7 ระเบิดเวลา (logic bomb) เป็นโปรแกรมอันตรายที่จะเริ่มทำงานโดยมีตัวกระตุ้นบางอย่างหรือกำหนดเงื่อนไขการทำงานบางอย่างขึ้นมา เช่น แอบส่งข้อมูลออกไปยังเครื่องอื่น หรือลบไฟล์ข้อมูลทิ้ง

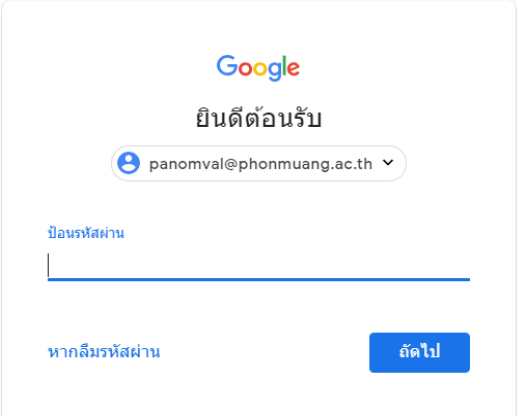
3.8 ประตูกล (backdoor/trapdoor) เป็นโปรแกรมที่มีการเปิดช่องโหว่ไว้เพื่อให้ผู้ไม่ประสงค์ดี สามารถเข้าไปคุกคามระบบสารสนเทศหรือเครื่องคอมพิวเตอร์ผ่านทางระบบเครือข่ายโดยที่ไม่มีใครรับรู้ บริษัทรับจ้างพัฒนาระบบสารสนเทศบางแห่งอาจจะติดตั้งประตูกลไว้เพื่อดึงข้อมูลหรือความลับของบริษัทโดยที่ผู้ว่าจ้างไม่ทราบ

1.2 วิธีการป้องกันภัยคุกคาม

วิธีการป้องกันภัยคุกคามด้านเทคโนโลยีสารสนเทศ จะต้องการตรวจสอบ และยืนยันตัวตนก่อนเริ่มใช้งาน โดยสามารถดำเนินการได้ 3 รูปแบบดังนี้

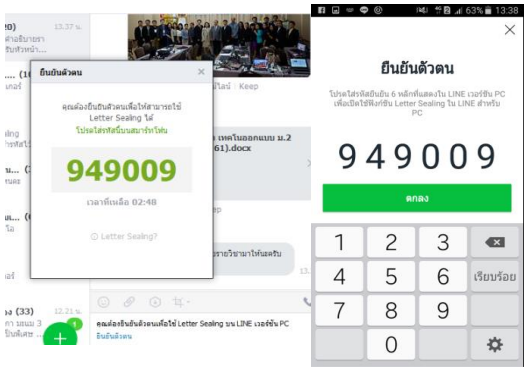
ตรวจสอบจากสิ่งที่ผู้ใช้รู้

เป็นการตรวจสอบตัวตนจากสิ่งที่ผู้ใช้งานรู้ข้อมูลของตนเองเพียงผู้เดียว เช่น ข้อมูลส่วนตัว บัญชีผู้ใช้และรหัสผ่าน เพราะข้อมูลเหล่านี้จะใช้เป็นข้อมูลที่นิยมในการตรวจสอบข้อมูล และมีระดับความปลอดภัยประโยชน์ในเวลาที่เราต้องการกู้คืนบัญชีใช้งาน ชื่อผู้ใช้และรหัสผ่าน



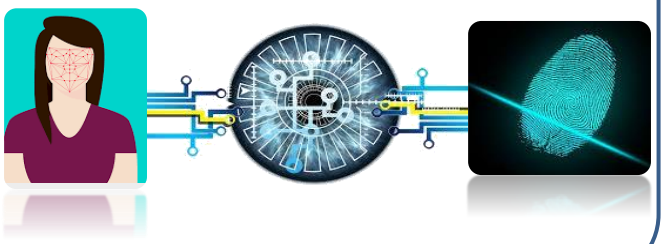
ตรวจสอบจากสิ่งที่ผู้ใช้มี

เป็นการตรวจสอบตัวตนจากอุปกรณ์ที่ใช้งานต้องมี เช่น บัตรสมาร์ตการ์ด บัตรเครดิต บัตรเอทีเอ็ม รหัสที่ตอบกลับมา เช่น การเข้าใช้งาน line pc จะมีรหัสให้เรายืนยันตัวตนที่โทรศัพท์มือถือ



ตรวจสอบจากสิ่งที่เป็นส่วนหนึ่งของผู้ใช้

เป็นการตรวจสอบข้อมูลชีวมาตร เช่น การสแกนนิ้วมือ ใบหน้า เสียง ม่านตา เป็นต้น การตรวจสอบแบบนี้มีประสิทธิภาพสูงสุด แต่บางส่วนอาจจะเห็นว่าเป็นการละเมิดสิทธิ์ความเป็นส่วนตัว



1.3 การตั้งรหัสผ่านให้ปลอดภัย

ในปัจจุบันการกำหนดรหัสผ่านเป็นวิธีการตรวจสอบตัวตนที่นิยมมาก เพราะช่วยในการรักษาความปลอดภัยของบัญชีผู้ใช้งานหรือในระบบที่ต้องการความปลอดภัย ช่วยป้องกันความปลอดภัย การเข้าถึงข้อมูลโดยมิชอบนั้นได้ หากผู้ใช้งานไม่ให้ความสำคัญในการตั้งค่ารหัสผ่านก็จะทำให้ผู้ไม่หวังดีสามารถคาดเดารหัสผ่านและเข้าถึงข้อมูลของท่านได้อย่างง่ายดาย สิ่งที่ควรคำนึงในการตั้งค่ารหัสผ่าน มีดังนี้

1. เป็นไปตามเงื่อนไขของระบบการใช้งาน ควรมีความยาวอย่างน้อย 8 ตัวอักษรหรือมากกว่านั้น ประกอบด้วยตัวอักษร (a-z, A-Z) ตัวเลข (0-9) เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
2. ไม่ควรนำข้อมูล ชื่อ นามสกุล เลขบัตรประจำตัวต่างๆ หรือวันเดือนปีเกิด เบอร์โทรศัพท์ มาตั้งเป็นรหัสผ่าน
3. ตั้งให้จดจำง่าย แต่ยากในการคาดเดา
4. ไม่ควรตั้งรหัสผ่านเหมือนกันทุกบัญชี
5. ไม่ควรบันทึกรหัสผ่านอัตโนมัติ
6. ไม่ควรเขียนรหัสผ่านลงในกระดาษหรือสมุดโน้ต
7. ควรเปลี่ยนรหัสผ่านของตนเองเป็นประจำ
8. ไม่บอกรหัสผ่านกับคนอื่น
9. ออกจากระบบทุกครั้งที่เลิกใช้งาน

2. การใช้เทคโนโลยีสารสนเทศให้ปลอดภัย

การเข้าใช้งานเทคโนโลยีสารสนเทศให้ปลอดภัย ต้องเรียนรู้และทำความเข้าใจเกี่ยวกับเงื่อนไขการใช้งานของระบบที่ให้บริการ ซึ่งทุกระบบมีการกำหนดเงื่อนไขการใช้งานทั้งสิ้น เงื่อนไขการใช้งานอาจจะถูกกำหนดด้วยข้อตกลงลักษณะต่างๆ ทำความเข้าใจเกี่ยวกับทรัพย์สินทางปัญญา เพื่อให้ใช้งานเทคโนโลยีสารสนเทศได้อย่างปลอดภัย

>> ลิขสิทธิ์ (Copyright)

ลิขสิทธิ์เป็นทรัพย์สินทางปัญญา (intellectual property) อย่างหนึ่ง ทรัพย์สินทางปัญญามีลักษณะพิเศษแตกต่างไปจากทรัพย์สินที่บัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ บรรพ 4 อันได้แก่ อสังหาริมทรัพย์และสังหาริมทรัพย์ กับสิทธิที่เกี่ยวกับทรัพย์สินดังกล่าว ลิขสิทธิ์เป็นสิทธิที่ไม่มีรูปร่าง กล่าวคือเป็นสิทธิหวงกันของเจ้าของที่ได้รับความคุ้มครองตามกฎหมาย เป็นสิทธิที่จะห้ามไม่ให้ผู้อื่นนำงานของเจ้าของไปใช้โดยไม่ได้รับอนุญาต อันมิใช่สิทธิในกรรมสิทธิ์หรือสิทธิครอบครอง ดังที่บัญญัติไว้ในประมวลกฎหมายแพ่งและพาณิชย์ เป็นสิทธิที่กฎหมายให้แก่ผู้สร้างสรรค์งานหรือผู้เป็นเจ้าของงานอันมีลิขสิทธิ์เท่านั้น ฉะนั้นผู้ เป็นเจ้าของกรรมสิทธิ์ในวัตถุมีรูปร่างจึงอาจจะไม่ใช่ผู้เป็นเจ้าของลิขสิทธิ์ก็เป็นได้

สัญญาอนุญาตครีเอทีฟคอมมอนส์
(Creative Commons Licence: CC)

เป็นสัญญาอนุญาตทางลิขสิทธิ์ประเภทหนึ่งพัฒนาโดย Hewlett Foundation study องค์กรไม่แสวงกำไรองค์กรหนึ่งที่เน้นงานด้านกฎหมาย วัตถุประสงค์ของสัญญานี้เพื่อให้เจ้าของผลงานอันมีลิขสิทธิ์สามารถแสดงข้อความอันอำนวยความสะดวกให้สาธารณชนรู้ถึงสิทธิ์ในผลงาน และทราบว่าจะนำงานอันมีลิขสิทธิ์ของตนไปใช้ได้โดยไม่ต้องขออนุญาตและไม่ถือว่าเป็นการละเมิดลิขสิทธิ์ โดยผู้ที่นำผลงานไปใช้ต้องปฏิบัติตามเงื่อนไขที่กำหนดไว้ เช่น อ้างอิงแหล่งที่มา ไม่ใช่เพื่อการค้า ไม่ดัดแปลงต้นฉบับ เป็นต้น รายละเอียดของแต่ละสัญญาอนุญาตนั้น ขึ้นอยู่กับรุ่นของสัญญา และประกอบไปด้วยตัวเลือกจากเงื่อนไข 4

ข้อกำหนดในการใช้ผลงานต่างๆ จะแทนด้วยสัญลักษณ์ ดังนี้

สัญลักษณ์	ข้อกำหนดในการใช้ผลงาน
	Attribution CC – BY ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มา
	Attribution CC – BY -SA ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มาและต้องเผยแพร่งานดัดแปลงโดยใช้สัญญาอนุญาตเดียวกัน
	Attribution CC – BY -ND ให้เผยแพร่ โดยต้องระบุที่มา แต่ห้ามดัดแปลง
	Attribution CC- BY -NC ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มาแต่ ห้ามใช้เพื่อการค้า
	Attribution CC- BY – NC – SA ให้เผยแพร่ ดัดแปลง โดยต้องระบุที่มาแต่ห้ามใช้เพื่อการค้าและต้องเผยแพร่งานดัดแปลงโดยใช้สัญญาอนุญาตชนิดเดียวกัน
	Attribution CC- BY – NC -ND ให้เผยแพร่ โดยต้องระบุที่มาแต่ห้ามดัดแปลงและห้ามใช้เพื่อการค้า

2.1 หลักการใช้อินเทอร์เน็ตอย่างปลอดภัย

ในปัจจุบันมีผู้ใช้บริการ บนระบบเครือข่ายอินเทอร์เน็ต ได้เพิ่มมากขึ้นเรื่อยๆทั่วโลก เพราะเป็นช่องทางที่สามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูลกันได้อย่างรวดเร็ว รวมถึงธุรกิจและพาณิชย์ในด้านต่างๆ ช่วยในเรื่องการลดระยะเวลาและต้นทุนในการติดต่อสื่อสาร แต่อย่างไรก็ตามผู้ใช้โดยทั่วไป ยังไม่เห็นความสำคัญ ของการใช้งานอินเทอร์เน็ตที่ปลอดภัยเท่าที่ควร เนื่องจากยังขาดความรู้ในการใช้งานและวิธีป้องกัน หรืออาจคิดว่าคงไม่มีปัญหาอะไรมาก ในการใช้งาน แต่เมื่อเกิดปัญหาขึ้นกับตัวเองแล้ว ก็ทำให้ตนเองเดือดร้อน เราสามารถป้องกันปัญหาเหล่านี้ได้ ดังนี้

1. ไม่ควรเปิดเผยข้อมูลส่วนตัว
2. ไม่ส่งหลักฐานส่วนตัวของตนเองและคนในครอบครัวให้ผู้อื่น เช่น สำเนาบัตรประชาชน เอกสารต่างๆ รวมถึงรหัสบัตรต่างๆ เช่น เอทีเอ็ม บัตรเครดิต ฯลฯ
3. ไม่ควรโอนเงินให้ใครอย่างเด็ดขาด นอกจากจะเป็นญาติสนิทที่เชื่อใจได้จริงๆ
4. ไม่ออกไปพบเพื่อนที่รู้จักทางอินเทอร์เน็ต เว้นเสียแต่ว่าได้รับอนุญาตจากพ่อแม่ผู้ปกครอง และควรมีผู้ใหญ่หรือเพื่อนไปด้วยหลายๆ คน เพื่อป้องกันการลักพาตัว หรือการกระทำมิดีมิร้ายต่างๆ
5. ระมัดระวังการซื้อสินค้าทางอินเทอร์เน็ต รวมถึงคำโฆษณาชวนเชื่ออื่นๆ เด็กต้องปรึกษาพ่อแม่ผู้ปกครอง โดยต้องใช้วิจารณญาณ พิจารณาความน่าเชื่อถือของผู้ขาย
6. สอนให้เด็กบอกพ่อแม่ผู้ปกครองหรือคุณครู ถ้าถูกกลั่นแกล้งทางอินเทอร์เน็ต
7. ไม่เผลอบันทึกข้อมูลผู้ใช้และรหัสผ่านขณะใช้เครื่องคอมพิวเตอร์สาธารณะ อย่าบันทึกผู้ใช้และรหัสผ่านของคุณบนเครื่องคอมพิวเตอร์นี้” อย่างเด็ดขาด เพราะผู้ที่มาใช้เครื่องต่อจากคุณ สามารถล็อคอินเข้าไป จากชื่อของคุณที่ถูกบันทึกไว้ แล้วสวมรอยเป็นคุณ หรือแม้แต่โอนเงินในบัญชีของคุณจ่ายค่าสินค้าและบริการต่างๆ ที่เขาต้องการ ผลก็คือคุณอาจหมดตัวและล้มละลายได้

8. ไม่ควรบันทึกภาพวิดีโอ หรือเสียงที่ไมเหมาะสมบนคอมพิวเตอร์ หรือบนมือถือ เพราะภาพ เสียง หรือวีดีโอนั้นๆ รั่วไหลได้ เช่นจากการแคร็ก ข้อมูล หรือถูกดาวน์โหลดผ่านโปรแกรม เพียร์ ทู เพียร์ (P2P) และถึงแม้ว่าคุณจะลบไฟล์นั้นออกไปจากเครื่องแล้ว ส่วนใดส่วนหนึ่งของไฟล์ยังตกค้างอยู่ แล้วอาจถูกกู้กลับขึ้นมาได้ โดยช่างคอม ช่างมือถือ

9. จัดการกับ Junk Mail จังค์ เมล์ หรือ อีเมล์ขยะปกติ การใช้อีเมล์จะมีกล่องจดหมายส่วนตัว หรือ Inbox กับ กล่องจดหมายขยะ Junk mail box หรือ Bulk Mail เพื่อแยกแยะประเภทของอีเมล์ เราจึงต้องทำความเข้าใจ และเรียนรู้ที่จะคัดกรองจดหมายอิเล็กทรอนิกส์ด้วยตัวเอง เพื่อกันไม่ให้มาปะปนกับจดหมายดีๆ ซึ่งเราอาจเผลอไปเปิดอ่าน แล้วถูกสปายแวร์ แอดแวร์เกาะติดอยู่บนเครื่อง หรือแม้แต่ติดไวรัสคอมพิวเตอร์

10. จัดการกับแอดแวร์ สปายแวร์ จัดการกับสปายแวร์แอดแวร์ที่ลักลอบเข้ามาสอดส่องพฤติกรรมการใช้เน็ตของคุณ ด้วยการซื้อโปรแกรมหรือไปดาวน์โหลดฟรีโปรแกรมมาดักจับและขจัดเจ้าแอดแวร์ สปายแวร์ออกไปจากเครื่องของคุณ ซึ่งสามารถดาวน์โหลดโปรแกรมฟรีได้ที่ แต่แค่มีโปรแกรมไว้ในเครื่องยังไม่พอ คุณต้องหมั่นอัพเดทโปรแกรมออนไลน์และสแกนเครื่องของคุณบ่อยๆด้วย เพื่อให้เครื่องของคุณปลอดสปาย ข้อมูลของคุณก็ปลอดภัย * โปรแกรมล้าง แอดแวร์ และ สปายแวร์ จะใช้โปรแกรมตัวเดียวกัน ซึ่งบางครั้งเขาอาจตั้งชื่อโดยใช้แค่เพียงว่า โปรแกรมล้าง แอดแวร์ แต่อันที่จริง มันลบทิ้งทั้ง แอดแวร์ และสปายแวร์พร้อมๆ กัน เพราะเจ้าสองตัวนี้ มันคล้ายๆ กัน

11. จัดการกับไวรัสคอมพิวเตอร์ คอมพิวเตอร์ทุกเครื่องจำเป็นต้องมีโปรแกรมสแกนดักจับและฆ่าไวรัส ซึ่งอันนี้ควรจะดำเนินการทันทีเมื่อซื้อเครื่องคอม เนื่องจากไวรัสพัฒนาเร็วมาก มีไวรัสพันธุ์ใหม่เกิดขึ้นทุกวัน แม้จะติดตั้งโปรแกรมฆ่าไวรัสไว้แล้ว ถ้าไม่ทำการอัพเดทโปรแกรมทางอินเทอร์เน็ต เวลาที่มีไวรัสตัวใหม่ๆ แอบเข้ามากับอินเทอร์เน็ต เครื่องคุณก็อาจจะโดนทำลายได้

12. ใช้ Adult Content Filter ในโปรแกรม P2P สำหรับผู้ชื่นชอบการดาวน์โหลดผ่านโปรแกรมแชร์ข้อมูล P2P ให้ระวังข้อมูลสำคัญ ไฟล์ภาพ วีดีโอส่วนตัว หรืออะไรที่ไม่ต้องการจะเปิดเผยสู่สาธารณะชน ควรบันทึกลงซีดี ดีวีดี หรือเทปไว้ อย่าเก็บไว้บนเครื่องคอมพิวเตอร์ เพราะคุณอาจถูกเจาะเอาข้อมูลเหล่านี้ไปได้

13. กรองเว็บไม่เหมาะสมด้วย Content Advisor ในอินเทอร์เน็ต เอ็กซ์พลอเรอในโปรแกรมเว็บ บราวเซอร์ อย่าง อินเทอร์เน็ต เอ็กซ์พลอเรอ ก็มีการตั้งค่า คอนเทนท์ แอดไวเซอร์ หรือฟังก์ชั่น การกรองเนื้อหาที่ไม่เหมาะสมสำหรับเด็ก ซึ่งจะทำให้เด็กไม่สามารถเปิดเข้าไปในเว็บไซต์ที่มีภาพและเนื้อหา โป๊ เปลือย ภาษาหยาบคาย รุนแรงได้ และยังมีการตั้งพาสเวิร์ด หรือรหัส สำหรับผู้ปกครอง เพื่อกันเด็กเข้าไปแก้ไขการตั้งค่าของคุณ ซึ่งคุณสามารถเข้าไปปลดล็อคได้ทุกเมื่อ ถ้าคุณจำเป็นต้องเข้าเว็บไซต์บางเว็บไซต์

2.2 พระราชบัญญัติ (พ.ร.บ.) ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560

พระราชบัญญัติ (พ.ร.บ.) ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 ฉบับล่าสุดได้มีการประกาศใช้เมื่อเดือนพฤษภาคม พ.ศ.2560 ซึ่งเป็น พ.ร.บ.คอมพิวเตอร์ ฉบับ 2 เพื่อการใช้เทคโนโลยีสารสนเทศอย่างถูกกฎหมาย สำหรับสาระสำคัญที่หลายคนควรพึงระวังใน พ.ร.บ.ว่าด้วยกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 หรือ พ.ร.บ.คอมพิวเตอร์ ฉบับ 2 มีสาระสำคัญจำง่ายๆ ดังนี้

1. การฝากร้านใน Facebook, IG ถือเป็นสแปม ปรับ 200,000 บาท

2. ส่ง SMS โฆษณา โดยไม่รับความยินยอม ให้ผู้รับสามารถปฏิเสธข้อมูลนั้นได้ ไม่เช่นนั้นถือเป็นสแปม ปรับ 200,000 บาท

3. ส่ง Email ขายของ ถือเป็นสแปม ปรับ 200,000 บาท

4. กด Like ได้ไม่ผิด พ.ร.บ.คอมพิวเตอร์ ยกเว้นการกดไลค์ เป็นเรื่องเกี่ยวกับสถาบัน เสี่ยงเข้าข่ายความผิดมาตรา 112 หรือมีความผิดร่วม

5. กด Share ถือเป็นการเผยแพร่ หากข้อมูลที่แชร์มีผลกระทบต่อผู้อื่น อาจเข้าข่ายความผิดตาม พ.ร.บ.คอมพิวเตอร์ โดยเฉพาะที่กระทบต่อบุคคลที่ 3

6. พบข้อมูลผิดกฎหมายอยู่ในระบบคอมพิวเตอร์ของเรา แต่ไม่ใช่สิ่งที่เจ้าของคอมพิวเตอร์กระทำเอง สามารถแจ้งไปยังหน่วยงานที่รับผิดชอบได้ หากแจ้งแล้วลบข้อมูลออกเจ้าของก็จะไม่มีความผิดตามกฎหมาย เช่น ความเห็นในเว็บไซต์ต่างๆ รวมไปถึงเฟซบุ๊ก ที่ให้แสดงความคิดเห็น หากพบว่าการแสดงความเห็นผิดกฎหมาย เมื่อแจ้งไปที่หน่วยงานที่รับผิดชอบเพื่อลบได้ทันที เจ้าของระบบเว็บไซต์จะไม่มีความผิด

7. สำหรับ แอดมินเพจ ที่เปิดให้มีการแสดงความเห็น เมื่อพบข้อความที่ผิด พ.ร.บ คอมพิวเตอร์ เมื่อลบออกจากพื้นที่ที่ตนดูแลแล้ว จะถือเป็นผู้พ้นผิด

8. ไม่โพสต์สิ่งลามกอนาจาร ที่ทำให้เกิดการเผยแพร่สู่ประชาชนได้

9. การโพสต์เกี่ยวกับเด็ก เยาวชน ต้องปิดบังใบหน้า ยกเว้นเมื่อเป็นการเชิดชู ชื่นชม อย่างให้เกียรติ

10. การให้ข้อมูลเกี่ยวกับผู้เสียชีวิต ต้องไม่ทำให้เกิดความเสื่อมเสียเชื่อเสียง หรือถูกดูหมิ่นเกลียดชัง ญาติสามารถฟ้องร้องได้ตามกฎหมาย

11. การโพสต์ด่าว่าผู้อื่น มีกฎหมายอาญาอยู่แล้ว ไม่มีข้อมูลจริง หรือถูกตัดต่อ ผู้ถูกกล่าวหาเอาผิดผู้โพสต์ได้ และมีโทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 200,000 บาท

12. ไม่ทำการละเมิดลิขสิทธิ์ผู้ใด ไม่ว่าข้อความ เพลง รูปภาพ หรือวิดีโอ

13. ส่งรูปภาพแชร์ของผู้อื่น เช่น สวัสดี อวยพร ไม่ผิด ถ้าไม่เอาภาพไปใช้ในเชิงพาณิชย์หารายได้