สรุปบทเรียน ที่ได้จากการพัฒนาความรู้

หลักสูตร : จริยธรรมการใช้เทคโนโลยีสารสนเทศ

Ethics for Using Information Technology

ผ่านแพลตฟอร์มเพื่อการเรียนรู้ออนไลน์ตลอดชีวิต
กระทรวงการอุดมศึกษา วิทยาศาสตร์ วิจัย
และนวัตกรรม (Thai MOOC) พัฒนาหลักสูตร
โดยภาควิชาเทคโนโลยีการศึกษา คณะศึกษาศาสตร์
มหาวิทยาลัยรามคำแหง

ผู้สอน : อาจารย์ ดร.บุษกร เชี่ยวจินดากานต์

จริยธรรมการใช้เทคโนโลยีสารสนเทศ
(Ethics for Using Information Technology)

1. ความเป็นส่วนตัว (Information Privacy)

ความเป็นส่วนตัว หมายถึง สิทธิในการควบคุมข้อมูลของตนเองที่เลือกจะเปิดเผยข้อมูลให้กับผู้อื่นหรือไม่ก็ได้

ลักษณะของข้อมูลส่วนบุคคล สามารถแบ่งได้เป็น 2 ประเภท

1) ข้อมูลเกี่ยวกับตัวบุคคล เป็นข้อมูลที่ใช้ยืนยันตัวตน ซึ่งได้แก่ หมายเลขบัตรประชาชน ประวัติการศึกษา ประวัติการทำงาน ประวัติครอบครัว ประวัติการรักษาพยาบาล ฐานะทางการเงิน พาสเวิร์ดสำหรับการเข้าถึงเว็บไซต์ต่าง ๆ ที่อยู่ในการสมัครสมาชิกเข้ารับบริการต่าง ๆ

2) ลักษณะเฉพาะของตัวบุคคล ได้แก่ รูปถ่าย ลายนิ้วมือ และน้ำเสียง

ประเภทของความเป็นส่วนตัวสามารถแบ่งเป็น 2 ประเภท

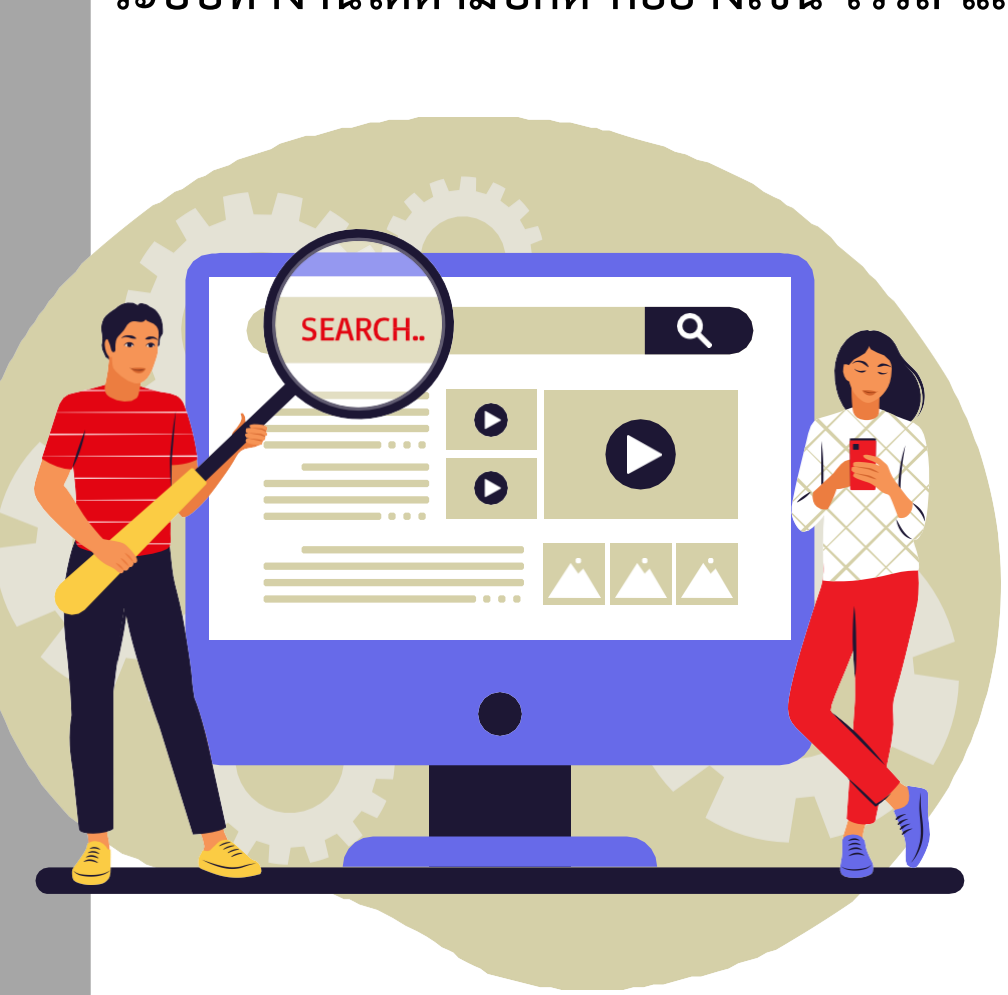
1) ความเป็นส่วนตัวทางด้านกายภาพ ซึ่งจะหมายถึงสิทธิในสถานที่ เวลา และสินทรัพย์ที่บุคคลพึงมี

2) ความเป็นส่วนตัวด้านสารสนเทศ ซึ่งจะหมายถึงข้อมูลทั่วไปเกี่ยวกับตัวบุคคล เช่น ชื่อ ที่อยู่ หมายเลขโทรศัพท์ หมายเลขบัตรเครดิต หรือว่าเลขที่บัญชีธนาคาร ที่บุคคลอื่นห้ามนำไปเปิดเผยหากไม่ได้รับอนุญาต

ประเภทภัยคุกคามความเป็นส่วนตัวในระบบคอมพิวเตอร์ สามารถแบ่งได้เป็น 2 ประเภท

1) อาชญากรรมคอมพิวเตอร์ โดยการใช้เทคโนโลยีคอมพิวเตอร์ และก็เน็ตเวิร์คเป็นเครื่องมือในการสร้างความเสียหายหรือก่ออาชญากรรมก็อย่างเช่น การสะกดรอยจากการใช้อินเทอร์เน็ต การล่อลวง การปลอมตัว หรือว่าการโจรกรรมอัตลักษณ์บุคคลสำหรับประเภทภัยคุกคามความเป็นส่วนตัว

2) การโจมตีคอมพิวเตอร์ ซึ่งมุ่งทำให้เกิดความเสียหายกับข้อมูลที่อยู่ในระบบคอมพิวเตอร์ และเน็ตเวิร์คโดยตรงเพื่อโจมตีไม่ให้ระบบทำงานได้ตามปกติ ก็อย่างเช่น ไวรัส และก็เวิร์มคอมพิวเตอร์



กรณีการกระทำผิดจริยธรรมการใช้เทคโนโลยีสารสนเทศด้านความเป็นส่วนตัว

1) การสะกดรอย (Cyber Stalking) การสะกดรอยในระบบเทคโนโลยีสารสนเทศก็คือการใช้เทคโนโลยีในการติดตามความเคลื่อนไหวหรือพฤติกรรมของบุคคล ตัวอย่างเช่น บริษัทใช้คอมพิวเตอร์ในการตรวจจับหรือเฝ้าดูการปฏิบัติงานของพนักงานถึงแม้ว่าจะเป็นการติดตามของพนักงานเพื่อพัฒนาคุณภาพงาน แต่กิจกรรมหลายอย่างของพนักงานก็ถูกเฝ้าดูไปด้วย ป้องกันได้โดยการไม่ Check-in ที่บ้านขณะอยู่คนเดียว ไม่ควรแชร์หรือเปิด Location Service ในโปรแกรม Chat และไม่ควรตั้งค่าการแชร์แบบสาธารณะ

2) การนำข้อมูลส่วนตัวของบุคคลอื่นไปขายให้กับผู้อื่น (Business Information Privacy) หากได้รับข่าวสารที่เป็นการละเมิดสิทธินั้นไม่ควรนำไปแชร์ต่อ แต่ควรแจ้งเจ้าหน้าที่ที่รับผิดชอบข้อมูลดำเนินการต่อไป

3) การโจรกรรมเอกลักษณ์บุคคล (Identity Theft) เกิดขึ้นเมื่อมีผู้ไม่หวังดีขโมยข้อมูลสำคัญที่ใช้ในการพิสูจน์เอกลักษณ์ของบุคคลอื่น เช่นชื่อและนามสกุล วันเดือนปีเกิด หมายเลขบัตรประชาชน หมายเลขหนังสือเดินทาง ใบขับขี่ รหัสบัตรเอทีเอ็ม หมายเลขบัตรเครดิต เป็นต้น เมื่อใดก็ตามที่ผู้กระทำผิดสามารถเข้าถึงข้อมูลส่วนบุคคลของผู้อื่นได้โดยนำข้อมูลของบุคคลอื่นไปใช้งาน โดยที่ไม่ได้รับความยินยอมจากเจ้าของข้อมูลนั้นก็ถือว่ามีความผิดทางจริยธรรม

4) การก่อกวนระบบสแปมเมล์ (Spam Mail) ก็คือการส่งจดหมายเวียนที่ผู้รับไม่ต้องการ ซึ่งทำให้เกิดอีเมลขยะและก็สร้างความรำคาญให้กับผู้รับ ส่วนใหญ่เป็นการโฆษณาหรือประชาสัมพันธ์เชิญชวนให้ซื้อสินค้าและบริการจะมาในรูปแบบของจดหมายอิเล็กทรอนิกส์ที่ส่งแบบหว่านแหให้กับผู้รับจำนวนมากในคราวเดียวกัน ซึ่งบางครั้งอาจมีการแนบไวรัส (Virus) หรือเวิร์ม (Worm) คอมพิวเตอร์ติดมาด้วยกับอีเมลนั้นด้วย

2. ความถูกต้อง (Information Accuracy)

ความถูกต้องในการใช้เทคโนโลยีสารสนเทศ ก็คือ การใช้เทคโนโลยีคอมพิวเตอร์ในการรวบรวม จับเก็บ เผยแพร่ และเรียกใช้ข้อมูลสารสนเทศ ซึ่งคุณลักษณะสำคัญประการหนึ่งก็คือ ความน่าเชื่อถือของข้อมูล ทั้งนี้ข้อมูลจะมีความน่าเชื่อถือถูกต้องเพียงใดย่อมขึ้นอยู่กับความถูกต้องในการบันทึกข้อมูลด้วย ประเด็นด้านความถูกต้องทางจริยธรรมโดยทั่วไป จะพิจารณาว่าใครเป็นผู้รับผิดชอบต่อข้อมูลที่จัดเก็บและเผยแพร่

กรณีการกระทำผิดจริยธรรมการใช้เทคโนโลยีสารสนเทศด้านความถูกต้อง

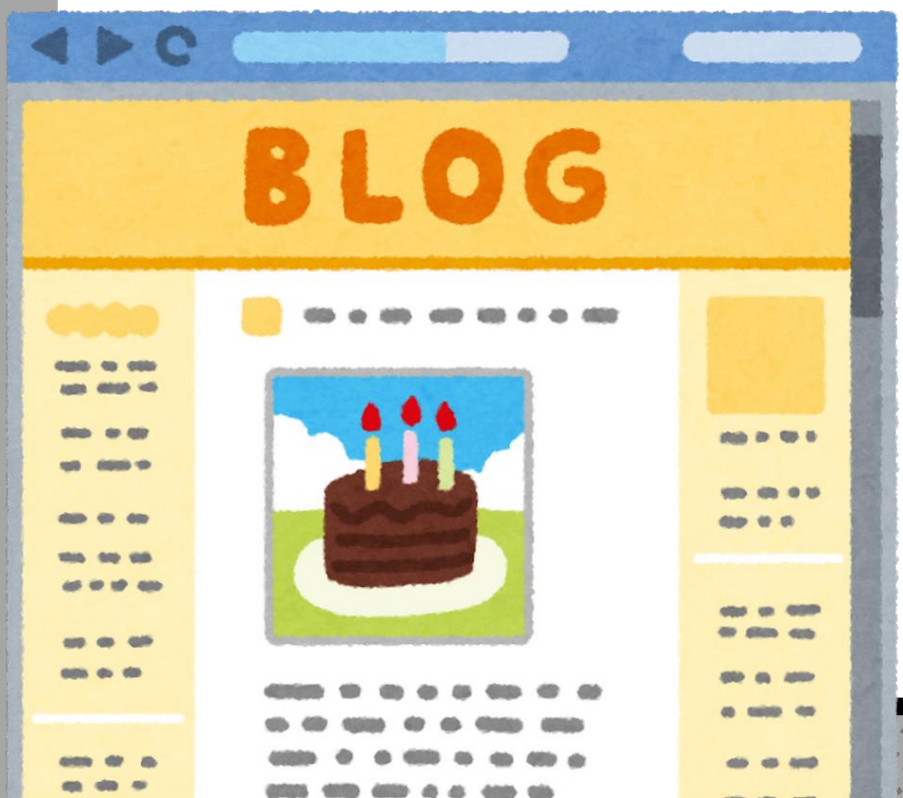
1) การสร้างความน่าเชื่อถือเทียม เป็นการโฆษณาชวนเชื่อของกลุ่มหนึ่ง ซึ่งเมื่อมีระบบคอมพิวเตอร์เข้ามา กลุ่มผู้ขายสินค้าก็อาจจะไปสร้างบทสนทนา บทความ หรือการนำเสนอรูปแบบอื่น ๆ ทำให้ผู้บริโภคหลงเชื่อ แนวทางการป้องกันคืออย่าสืบค้นข้อมูลแค่บางเว็บไซต์เท่านั้น แต่ควรหาข้อมูลจากเว็บไซต์อื่น ๆ หรือสื่ออื่น ๆ ประกอบด้วย

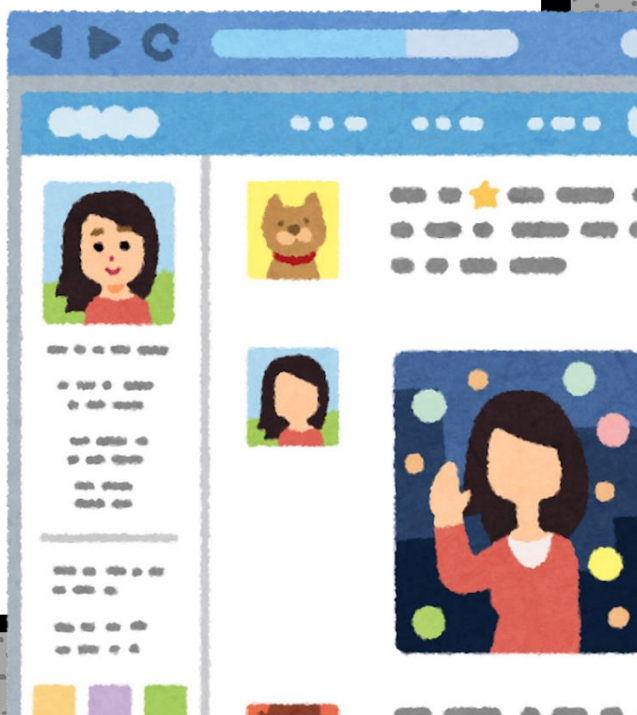
2) เสรีภาพในการแสดงความคิดเห็น ซึ่งอาจเป็นการแสดงความคิดเห็นที่ไม่เหมาะสมและความคิดเห็นที่กฎหมายไม่คุ้มครอง เช่น คำลามก อนาจาร คำใส่ร้ายป้ายสี คำยั่วยุให้เกิดความกลัว คำยั่วยุให้มีการก่ออาชญากรรม คำดูถูกเหยียดหยาม คำปลุกปั่นก่อให้เกิดความไม่สงบหรือก่อจลาจล การป้องกันควรจำกัดการเข้าถึงของเยาวชน การตรากฎหมายขึ้นมาเพื่อควบคุม

กรณีการกระทำผิดจริยธรรมการใช้เทคโนโลยีสารสนเทศด้านความถูกต้อง (ต่อ)

3) การหลอกลวง ซึ่งอาจเป็นการสร้างข่าวหลอกลวง หรือการหลอกลวงด้วยเว็บไซต์ปลอม หรือ Phishing คือ การสร้างหน้าเว็บเพจปลอมที่คล้ายคลึงกับเว็บเพจจริง แต่จะมีข้อความหรือรูปภาพบางอย่างที่ไม่เหมือนกัน จุดที่ต้องสังเกตก็คือ ตำแหน่งที่ตั้งของไฟล์ที่เรียกว่า URL จะมีความคล้ายคลึงหรือแตกต่างกันเล็กน้อย เช่น เว็บไซต์ของการเข้าไปใช้บริการของธนาคาร การเข้าถึงเว็บไซต์ปลอมอาจจะเกิดจากความบังเอิญของผู้ใช้งาน หรือการเข้าถึงจากคำค้นข้อมูลต่าง ๆ บนระบบอินเทอร์เน็ต จุดประสงค์หลักก็เพื่อจะเอาข้อมูลของผู้ใช้งานไปใช้ประโยชน์ต่อไป ส่วนใหญ่เป็นข้อมูลส่วนตัว ข้อมูลที่เกี่ยวข้องกับบัตรเครดิต เลขที่บัญชี รหัสผ่านธนาคาร แนวทางการป้องกันการกระทำผิดจริยธรรม ในการหลอกลวงด้วยเว็บไซต์ปลอมก็คือ เราควรสังเกตความผิดปกติจากการสำรวจชื่อเว็บไซต์ ตำแหน่งที่ตั้งของไฟล์ หรือ URL รายละเอียดในเว็บเพจว่าน่าเชื่อถือหรือไม่ ลองเข้าเว็บไซต์ด้วยการป้อนหมายเลขไอพี หรือเข้าเว็บไซต์ผ่านผลของการสืบค้นทางอินเทอร์เน็ต

4) การเผยแพร่ข้อมูลโดยไม่มีแหล่งที่มา ในยุคที่มีการแชร์และการส่งข้อมูลต่อ ๆ กันอย่างรวดเร็วนั้น อาจจะขาดการกลั่นกรองจากผู้รับสาร ไม่มีแหล่งที่มาที่น่าเชื่อถือ ข้อมูลถูกบิดเบือนส่งผลทำให้เกิดความเข้าใจผิด หรือมีเนื้อหาไม่เหมาะสม ดังนั้นจึงควรตรวจสอบข้อมูลให้ดีก่อนแชร์ไปให้ผู้อื่น





3. ความเป็นเจ้าของ (Information Property)

ความเป็นเจ้าของในการใช้เทคโนโลยีสารสนเทศ คือกรรมสิทธิ์ในการถือครองทรัพย์สินซึ่งทรัพย์สินเหล่านี้จะได้รับความคุ้มครองสิทธิภายใต้กฎหมาย โดยสามารถแบ่งได้เป็น 2 ประเภท

1) ทรัพย์สินที่จับต้องได้ เช่น คอมพิวเตอร์ รถยนต์ อสังหาริมทรัพย์

2) ทรัพย์สินที่จับต้องไม่ได้ แต่สามารถถ่ายทอดและบันทึกลงในสื่อต่าง ๆ ได้ เช่น บทเพลง ภาพยนตร์ โปรแกรมคอมพิวเตอร์ เราเรียกทรัพย์สินประเภทนี้ว่าทรัพย์สินทางปัญญา ทรัพย์สินทางปัญญาเป็นผลงานอันเกิดจากการ คิดค้น หรือสร้างสรรค์ของบุคคลจนเป็นสิ่งประดิษฐ์ขึ้นมา ผู้ที่เป็นเจ้าของทรัพย์สินซึ่งถือเป็นผู้ที่มี “สิทธิในการเป็นเจ้าของ” ซึ่งเป็น “สิทธิตามธรรมชาติ” ที่บุคคลพึงมี และบุคคลนั้นย่อมสมควรที่จะได้รับผลประโยชน์จากทรัพย์สินทางปัญญาที่เป็นผลงานของตน หากบุคคลใดนำทรัพย์สินทางปัญญาของบุคคลอื่นไปใช้เพื่อแสวงหาประโยชน์ให้แก่ตน โดยไม่ได้รับอนุญาตจากเจ้าของ ก็จัดว่าเป็นการนำไปใช้อย่างไม่ชอบธรรม เป็นเหตุให้เจ้าของทรัพย์สินไม่ได้รับประโยชน์จากผลงานของตน และเพื่อเป็นการคุ้มครองผู้เป็นเจ้าของทรัพย์สินทางปัญญาในแต่ละประเทศจึงได้มีการตรากฎหมายขึ้นมา และสำหรับประเทศไทยนั้นจะมีหน่วยงานที่ดูแลในด้านความเป็นเจ้าของในการใช้เทคโนโลยีสารสนเทศ เช่น กรมทรัพย์สินทางปัญญา กระทรวงพาณิชย์ ก็จะดูแลในเรื่องของลิขสิทธิ์ สิทธิบัตรเครื่องหมายการค้า สิ่งบ่งชี้ทางภูมิศาสตร์ต่าง ๆ ทรัพย์สินประเภทนี้ได้แก่ ลิขสิทธิ์ เครื่องหมายการค้า คลามลับทางการค้า สิทธิบัตร และอนุสิทธิบัตร

กรณีการกระทำผิดจริยธรรมการใช้เทคโนโลยีสารสนเทศด้านความเป็นเจ้าของ

1) การละเมิดทรัพย์สินทางปัญญา เช่น การคัดลอก ทำซ้ำ จำหน่าย จ่ายแจก หรือเผยแพร่ผลงานของผู้อื่นโดยไม่ได้ขออนุญาตหรือจ่ายค่าลิขสิทธิ์ให้กับเจ้าของ อย่างเช่น การคัดลอกภาพยนตร์เพื่อจำหน่ายหรือเผยแพร่ ทำให้บริษัทภาพยนตร์สูญเสียรายได้ ดังนั้น การได้รับความคุ้มครองลิขสิทธิ์ จึงเป็นการควบคุมไม่ให้ผู้อื่นกระทำการใด ๆ ที่ถือได้ว่าเป็นการละเมิดลิขสิทธิ์

2) การละเมิดลิขสิทธิ์ซอฟแวร์ การที่บุคคลจะสามารถนำซอฟแวร์ของผู้อื่นไปใช้งานได้อย่างถูกต้องตามกฎหมายนั้นจะต้องได้รับอนุญาตจากเจ้าของลิขสิทธิ์ หรือจ่ายค่าลิขสิทธิ์แล้วเท่านั้น การกระทำที่ถือว่าเป็นการละเมิด ได้แก่ การคัดลอก ทำซ้ำโปรแกรคอมพิวเตอร์ให้กับบุคคลอื่น หรือคัดลอกโปรแกรมคอมพิวเตอร์ของบุคคลอื่นมาใช้งาน รวมถึงการแสวงหากำไรในรูปแบบต่าง ๆ จากซอฟแวร์ที่มีลิขสิทธิ์ เช่น การขาย การให้เช่า การเผยแพร่ต่อสาธารณชน การแจกจ่ายในลักษณะที่ก่อให้เกิดความเสียหายแก่เจ้าของลิขสิทธิ์

3) การขโมยความคิด คือ การที่บุคคลขโมยความคิดและคำพูดของบุคคลอื่นมาเป็นงานของตน เราเรียกว่า การโจรกรรมผลงานการขโมยความคิดหรือผลงานของผู้อื่นเป็นประเด็นที่มีการกล่าวถึงและให้ความสำคัญมากขึ้นโดยเฉพาะแวดวงในการทำวิจัยและวิทยานิพนธ์ในสถาบันการศึกษาต่าง ๆ ทั้งในประเทศและต่างประเทศเนื่องจากแหล่งการสืบค้นงานวิจัยและบทความต่าง ๆ นั้น สามารถเข้าถึงได้โดยง่ายจากเครือข่ายอินเทอร์เน็ตดังนั้นจึงควรระมัดระวัง เมื่อต้องนำข้อความหรือผลงานของผู้อื่นมาใช้งานโดยจะต้องอ้างอิงเจ้าของผลงานนั้นด้วยมิฉะนั้นจะถือว่าเป็นการละเมิดลิขสิทธิ์ ซึ่งจัดได้ว่าเป็นการโจรกรรมทรัพย์สินทางปัญญาและเป็นการกระทำที่ผิดจรรยาบรรณสถาบันการศึกษาต่าง ๆ จึงมีบทลงโทษที่ค่อนข้างรุนแรง

4. การเข้าถึงข้อมูล (Data Accessibility)

การเข้าถึงข้อมูล หมายถึง สิทธิ์ในการเข้าถึงข้อมูลของตนเองและของผู้อื่น ซึ่งการเข้าใช้งานโปรแกรมหรือระบบคอมพิวเตอร์มักจะมีการกำหนดสิทธิ์ตามระดับของผู้ใช้งาน เพื่อป้องกันการเข้าไปดำเนินการต่าง ๆ กับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้องและก็เป็นการรักษาความปลอดภัยของข้อมูลด้วย ดังนั้นในการพัฒนาระบบคอมพิวเตอร์จึงได้มีการออกแบบระบบรักษาความปลอดภัยในการเข้าถึงข้อมูลของผู้ใช้งาน ซึ่งการเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอมก็ถือว่าเป็นการกระทำผิดเช่นเดียวกับการละเมิดสิทธิ์ความเป็นส่วนตัว

การกำหนดสิทธิ์ตามระดับผู้ใช้งาน ก็คือ การกำหนดสิทธิ์ให้กับบุคคลในการเข้าถึงข้อมูลเพื่อเข้าไปดำเนินการใด ๆ กับข้อมูลที่ตนเองเกี่ยวข้อง ตัวอย่างสิทธิ์ในการเข้าใช้งานระบบอย่างเช่นให้สิทธิ์ในการบันทึก มีสิทธิ์ในการแก้ไขหรือว่าสิทธิ์ในการลบข้อมูล ตัวอย่างของการกำหนดสิทธิ์ตามระดับของผู้ใช้งาน ถ้ากำหนดให้เป็นผู้มีสิทธิ์ดำเนินการได้ก็คือ เป็นผู้ที่เข้าไปตรวจสอบและก็แก้ไขความถูกต้องของข้อมูลในระบบได้ อย่างเช่น แอดมินสามารถเข้าไปกระทำการใด ๆ กับข้อมูลนั้นก็ได้ แต่ก็ต้องมีแนวทางปฏิบัติหรือว่าการบันทึกการทำงานที่สามารถตรวจสอบได้ เพื่อไม่ให้ละเมิดสิทธิ์ความเป็นส่วนตัว

กรณีการกระทำผิดจริยธรรมการใช้เทคโนโลยีสารสนเทศ ด้านการเข้าถึงข้อมูล

1) การลักลอบเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การลักลอบการเข้าถึงข้อมูลในระบบเทคโนโลยีสารสนเทศก็คือ การลักลอบเข้าไปดูข้อมูลของบุคคลอื่นที่บันทึกลงในเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาต ซึ่งการกระทำผิดที่เราเห็นได้บ่อยเป็นการเข้าไปอ่านจดหมายอิเล็กทรอนิกส์ หรือว่าอีเมล์ของผู้อื่น ซึ่งถือเป็นการสร้างความเสียหายต่อบุคคลและสังคมสารสนเทศเป็นอย่างมาก สามารถป้องกันได้ด้วยการ Logout จากเครื่องคอมพิวเตอร์ทุกครั้ง หรือการตั้งรหัสผ่านที่ไม่สามารถคาดเดาได้ง่ายจนเกิดไป การกำหนดการเข้าถึงข้อมูลด้วยการสแกนลายนิ้วมือหรือการสแกนม่านตา

2) การใช้โปรแกรมคอมพิวเตอร์ที่ไม่เป็นมิตร (Malware) โปรแกรมคอมพิวเตอร์ที่ไม่เป็นมิตรนี้คือชุดคำสั่งอันตรายที่แอบแฝงมากับไฟล์หรืออีเมล์ เมื่อเข้าสู่ระบบคอมพิวเตอร์ของเราแล้วก็จะสามารถทำงานได้หลายลักษณะ โปรแกรมประสงค์ร้ายหรือโปรแกรมที่ไม่เป็นมิตรนี้ก็จะมีดังนี้

- ไวรัสคอมพิวเตอร์ ก็คือโปรแกรมหรือชุดคำสั่งที่ไม่ประสงค์ดี แพร่กระจายไปได้ด้วยตัวเอง เขียนโดยนักพัฒนาโปรแกรมที่มีความชำนาญเฉพาะด้าน

- เวิร์มหรือหนอนอินเทอร์เน็ต เป็นโปรแกรมเคลื่อนที่ไปในระบบเครือข่ายได้เองโปรแกรมมีความรุนแรงกว่าไวรัสคอมพิวเตอร์แบบเดิมมากจะทำลายระบบทรัพยากรคอมพิวเตอร์ให้มีประสิทธิภาพลดลงและไม่อาจทำงานต่อไปได้

- ม้าโทรจันหรือที่เราเรียกว่า โทรจัน คือโปรแกรมที่แอบทำงานลับ ๆ ด้วยการเปิดให้มีการบุกรุกเข้าสู่ระบบได้ง่ายโดยอาศัยการฝังตัวอยู่ในระบบคอมพิวเตอร์เครื่องนั้น และจะไม่มีการแพร่กระจายตัวแต่อย่างใด โปรแกรมจะถูกตั้งเวลาการทำงานหรือควบคุมการทำงานจากระยะไกลโดยผู้ไม่ประสงค์ดี เพื่อให้เข้ามาดำเนินการต่าง ๆ ในเครื่องคอมพิวเตอร์เป้าหมายได้ แนวทางการป้องกันก็คือการใช้โปรแกรมป้องกันไวรัสและทำการ Update อยู่เสมอ การใช้ระบบไฟร์วอลล์ของคอมพิวเตอร์ และอาจมีการสำรองข้อมูลอยู่เสมอ โดยเฉพาะข้อมูลที่สำคัญ

ประโยชน์ที่ได้รับ

ในยุคที่ข้อมูลส่วนตัวของทุกคนล้วนอยู่บนระบบคอมพิวเตอร์และอินเตอร์เน็ตทั้งสิ้น เราในฐานะเจ้าของข้อมูลควรที่จะศึกษาหาความรู้เกี่ยวกับเรื่องการโจรกรรมข้อมูลเอาไว้ และหากจำเป็นที่ข้อมูลส่วนตัวจะต้องอยู่บนระบบคอมพิวเตอร์ หรืออินเตอร์เน็ต ก็ควรที่จะมีการตั้งรหัสผ่านการเข้าถึงข้อมูลที่ยากต่อการคาดเดา เพื่อป้องกันการโจรกรรมข้อมูล เจ้าหน้าที่ที่มีสิทธิเข้าถึงข้อมูลส่วนตัวของผู้อื่นก็ควรมีจริยธรรม โดยการไม่แอบเอาข้อมูลส่วนตัวของผู้อื่นไปเปิดเผย และที่สำคัญคือการเข้าใช้อินเตอร์เน็ตในปัจจุบันนั้นต้องใช้ความระมัดระวังเป็นอย่างมาก เนื่องจากมีมิจฉาชีพทำเว็บไซต์ปลอมมากมาย หากเราตกเป็นเหยื่ออาจทำให้สูญเสียทั้งข้อมูลส่วนตัวและทรัพย์สินก็เป็นได้

นางสาวกลวัชร ยุติธรรมดำรง
นิติกรปฏิบัติการ
กลุ่มวินัย กองการเจ้าหน้าที่ กรมพัฒนาที่ดิน
สิงหาคม 2567