แบบรายงานผลการพัฒนาความรู้ของข้าราชการ สพข.๗
รอบการประเมิน ๑ (ตุลาคมคม ๒๕๖๘ - มีนาคม ๒๕๖๙)
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ชื่อ – นามสกุล : ว่าที่ร.ต.พงษ์อนันต์ นามวงศ์ **ตำแหน่ง :** นายช่างโยธาชำนาญงาน
กลุ่ม/ฝ่าย กลุ่มสำรวจเพื่อทำแผนที่
หลักสูตร/หัวข้อเรื่องอบรม/สัมมนา/พัฒนาความรู้ฯ : ความเข้าใจการบริหารความเสี่ยง
สถานที่อบรม/สัมมนา/พัฒนาความรู้ฯ : ระบบการอบรมผ่านสื่ออิเล็คทรอนิกส์ LDD e -Training ของกรมพัฒนาที่ดิน
หน่วยงานที่จัดฝึกอบรม/สัมมนา/พัฒนาความรู้ฯ : กองคลัง กรมพัฒนาที่ดิน
วันที่ ๕ กุมภาพันธ์ ๒๕๖๙
วิทยากร : ดร.โษฑศ์รัตต ธรรมบุษดี IT Management Of Engineering, Mahidol University
ดร.ทวีศักดิ์ สมานชื่น คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล
จิราภาส อุดปวง นักวิชาการพัสดุปฏิบัติการ

จริยธรรมการใช้เทคโนโลยีสารสนเทศ

จริยธรรมการใช้เทคโนโลยีสารสนเทศ หมายถึง หลักความประพฤติที่ถูกต้องเหมาะสมในการใช้เทคโนโลยีและระบบสารสนเทศ เพื่อไม่ให้เกิดความเสียหายต่อตนเองและผู้อื่น ในปัจจุบันเทคโนโลยีสารสนเทศมีบทบาทสำคัญในชีวิตประจำวัน ทั้งด้านการศึกษา การทำงาน และการสื่อสาร ดังนั้นผู้ใช้จึงควรมีจิตสำนึกและความรับผิดชอบในการใช้งาน

การใช้เทคโนโลยีสารสนเทศอย่างมีจริยธรรม ได้แก่ การไม่ละเมิดสิทธิส่วนบุคคลของผู้อื่น ไม่คัดลอกหรือเผยแพร่ข้อมูลที่เป็นเท็จหรือผิดกฎหมาย ไม่ละเมิดลิขสิทธิ์ผลงานของผู้อื่น เช่น การคัดลอกผลงานหรือโปรแกรมโดยไม่ได้รับอนุญาต รวมถึงการใช้ข้อมูลและสื่อออนไลน์อย่างเหมาะสม

นอกจากนี้ ผู้ใช้ควรคำนึงถึงความปลอดภัยของข้อมูล ไม่เปิดเผยข้อมูลส่วนตัวของตนเองและผู้อื่นโดยไม่จำเป็น รวมถึงการใช้งานสื่อสังคมออนไลน์อย่างมีสติ เคารพความคิดเห็นที่แตกต่าง และไม่ใช้เทคโนโลยีไปในทางที่ก่อให้เกิดความเสียหายต่อสังคม

จริยธรรมการใช้งานคอมพิวเตอร์ (PAPA)

จริยธรรมการใช้งานคอมพิวเตอร์ (PAPA) เป็นแนวคิดด้านจริยธรรมสารสนเทศที่ใช้เป็นหลักในการพิจารณาการใช้คอมพิวเตอร์อย่างเหมาะสม โดยคำว่า PAPA ประกอบด้วยองค์ประกอบสำคัญ 4 ประการ ได้แก่ Privacy, Accuracy, Property และ Accessibility ซึ่งช่วยกำหนดแนวทางในการใช้งานคอมพิวเตอร์อย่างมีความรับผิดชอบ

1. **Privacy (ความเป็นส่วนตัว)** หมายถึง การเคารพสิทธิความเป็นส่วนตัวของผู้อื่น ผู้ใช้งานไม่ควรเข้าถึง เปิดเผย หรือใช้ข้อมูลส่วนบุคคลของผู้อื่นโดยไม่ได้รับอนุญาต

2. **Accuracy (ความถูกต้องของข้อมูล)** หมายถึง ความรับผิดชอบในการใช้และเผยแพร่ข้อมูลที่ถูกต้อง ไม่บิดเบือนข้อมูล หรือเผยแพร่ข้อมูลที่เป็นเท็จซึ่งอาจก่อให้เกิดความเสียหายแก่ผู้อื่น

3. **Property (ความเป็นเจ้าของ)** หมายถึง การเคารพลิขสิทธิ์และทรัพย์สินทางปัญญา ผู้ใช้งานไม่ควรคัดลอก ดัดแปลง หรือเผยแพร่ผลงานของผู้อื่นโดยไม่ได้รับอนุญาตหรือไม่อ้างอิงแหล่งที่มา

4. **Accessibility (การเข้าถึงข้อมูล)** หมายถึง การใช้สิทธิในการเข้าถึงข้อมูลอย่างเหมาะสม ไม่เข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต และไม่กีดกันผู้อื่นจากการเข้าถึงข้อมูลที่ควรได้รับ

บัญญัติ 10 ประการของการใช้อินเทอร์เน็ต

1. **ไม่ใช้คอมพิวเตอร์ทำร้ายผู้อื่น** ไม่ใช้คอมพิวเตอร์หรืออินเทอร์เน็ตเพื่อกลั่นแกล้ง หลอกลวง หรือสร้างความเสียหายให้แก่ผู้อื่น
2. **ไม่รบกวนการทำงานของผู้อื่น** ไม่กระทำการที่ก่อให้เกิดความเดือดร้อน เช่น ส่งไวรัส หรือแฮกระบบของผู้อื่น
3. **ไม่สอดแนมหรือเข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาต** เคารพสิทธิส่วนบุคคลและความเป็นส่วนตัวของผู้อื่น
4. **ไม่ใช้อินเทอร์เน็ตเพื่อการโจรกรรม** ไม่ขโมยข้อมูล ทรัพย์สิน หรือเงินของผู้อื่นผ่านระบบออนไลน์
5. **ไม่ใช้อินเทอร์เน็ตเพื่อเผยแพร่ข้อมูลเท็จ** ไม่บิดเบือนข้อมูลหรือเผยแพร่ข่าวปลอมที่อาจสร้างความเสียหาย
6. **ไม่คัดลอกหรือใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์** เคารพทรัพย์สินทางปัญญาและผลงานของผู้อื่น
7. **ไม่ใช้ทรัพยากรของผู้อื่นโดยไม่ได้รับอนุญาต** เช่น การใช้บัญชีอินเทอร์เน็ตหรือข้อมูลของผู้อื่นโดยไม่ได้รับความยินยอม
8. **ไม่นำผลงานของผู้อื่นมาเป็นของตนเอง** ต้องอ้างอิงแหล่งที่มาเมื่อใช้ข้อมูลหรือผลงานของผู้อื่น
9. **คำนึงถึงผลกระทบทางสังคมจากการใช้อินเทอร์เน็ต** ใช้เทคโนโลยีอย่างมีสติและรับผิดชอบต่อสังคม
10. **ใช้อินเทอร์เน็ตด้วยความเคารพและมีมารยาท** ปฏิบัติต่อผู้อื่นอย่างสุภาพ ให้เกียรติ และไม่ละเมิดสิทธิของผู้อื่น

พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2558

พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2558 เป็นกฎหมายที่แก้ไขเพิ่มเติมจาก พ.ร.บ.ลิขสิทธิ์ พ.ศ. 2537 เพื่อให้สอดคล้องกับการใช้งานผลงานในยุคดิจิทัลและอินเทอร์เน็ต โดยมุ่งเน้นการคุ้มครองสิทธิของเจ้าของผลงาน และคุ้มครองผู้ใช้งานโดยสุจริต

สาระสำคัญของ พ.ร.บ. ลิขสิทธิ์ 2558

1. คุ้มครองผลงานลิขสิทธิ์ในรูปแบบดิจิทัล เช่น งานออนไลน์ เว็บไซต์ และสื่ออิเล็กทรอนิกส์
2. เพิ่มมาตรการคุ้มครองเจ้าของลิขสิทธิ์จากการละเมิดบนอินเทอร์เน็ต
3. กำหนดความรับผิดของผู้ให้บริการอินเทอร์เน็ต (ISP) หากเพิกเฉยต่อการละเมิด
4. อนุญาตให้ศาลมีอำนาจสั่งระงับการละเมิดลิขสิทธิ์ได้อย่างรวดเร็ว
5. คุ้มครองการใช้ผลงานโดยสุจริต (Fair Use) เช่น เพื่อการศึกษา วิจัย หรือไม่แสวงหากำไร
6. ไม่ถือว่าการดาวน์โหลดเพื่อใช้ส่วนตัวเป็นความผิดทางอาญา แต่ยังอาจเป็นความผิดทางแพ่ง
7. ห้ามทำซ้ำ ดัดแปลง หรือเผยแพร่ผลงานโดยไม่ได้รับอนุญาต
8. โปรแกรมคอมพิวเตอร์ได้รับความคุ้มครองตามกฎหมายลิขสิทธิ์
9. ผู้ละเมิดลิขสิทธิ์มีโทษทั้งจำคุก ปรับ หรือทั้งจำทั้งปรับ
10. ส่งเสริมการเคารพลิขสิทธิ์และทรัพย์สินทางปัญญาในสังคมดิจิทัล

พระราชบัญญัติลิขสิทธิ์ (สรุป 12 ข้อ)

1. ลิขสิทธิ์เป็นสิทธิของผู้สร้างสรรค์ผลงานโดยชอบด้วยกฎหมาย
2. ผลงานที่ได้รับความคุ้มครอง ได้แก่ งานเขียน งานดนตรี งานศิลปกรรม งานภาพยนตร์ และโปรแกรมคอมพิวเตอร์
3. เจ้าของลิขสิทธิ์มีสิทธิแต่เพียงผู้เดียวในการทำซ้ำ ดัดแปลง และเผยแพร่ผลงาน
4. ห้ามคัดลอกหรือทำซ้ำผลงานของผู้อื่นโดยไม่ได้รับอนุญาต
5. การละเมิดลิขสิทธิ์ถือเป็นความผิดตามกฎหมาย
6. การอ้างอิงแหล่งที่มาอย่างถูกต้องเป็นสิ่งที่ควรปฏิบัติ
7. การใช้ผลงานเพื่อการศึกษาอาจทำได้ในขอบเขตที่กฎหมายอนุญาต
8. ห้ามจำหน่าย เผยแพร่ หรือแสวงหาผลประโยชน์จากผลงานที่ละเมิดลิขสิทธิ์
9. โปรแกรมคอมพิวเตอร์ถือเป็นผลงานที่ได้รับความคุ้มครองตามกฎหมายลิขสิทธิ์
10. การดัดแปลงผลงานต้องได้รับอนุญาตจากเจ้าของลิขสิทธิ์
11. ผู้ละเมิดลิขสิทธิ์ต้องรับโทษทั้งทางแพ่งและทางอาญา
12. การเคารพลิขสิทธิ์ช่วยส่งเสริมการสร้างสรรค์ผลงานและพัฒนาสังคม

หลัก 3 ประการของการไม่ละเมิดลิขสิทธิ์

1. ขออนุญาต
2. ห้ามดัดแปลง
3. ให้เครดิต

ลิขสิทธิ์และบริการด้านสารสนเทศ

ลิขสิทธิ์เป็นสิทธิทางกฎหมายที่คุ้มครองผู้สร้างสรรค์ผลงานทางปัญญา เช่น หนังสือ บทความ งานวิจัย สื่อดิจิทัล และโปรแกรมคอมพิวเตอร์ เพื่อป้องกันการนำผลงานไปใช้ คัดลอก หรือเผยแพร่โดยไม่ได้รับอนุญาต ส่วนบริการด้านสารสนเทศ คือ การให้บริการข้อมูลข่าวสารแก่ผู้ใช้ เช่น ห้องสมุด ศูนย์สารสนเทศ ฐานข้อมูลออนไลน์ และระบบห้องสมุดดิจิทัล การให้บริการด้านสารสนเทศจำเป็นต้องคำนึงถึงกฎหมายลิขสิทธิ์อย่างเคร่งครัด เพื่อให้การใช้ข้อมูลเป็นไปอย่างถูกต้องตามกฎหมาย ผู้ให้บริการต้องจัดหาทรัพยากรสารสนเทศที่ถูกลิขสิทธิ์ และกำหนดแนวทางการใช้ที่เหมาะสมแก่ผู้ใช้บริการผู้ใช้บริการสารสนเทศควรใช้ข้อมูลอย่างมีจริยธรรม เช่น การอ้างอิงแหล่งที่มาเมื่อใช้ข้อมูลหรือผลงานของผู้อื่น ไม่คัดลอกผลงานทั้งหมดมาเป็นของตนเอง และไม่เผยแพร่หรือจำหน่ายผลงานที่มีลิขสิทธิ์โดยไม่ได้รับอนุญาต

สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights)

สิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights: IPR) หมายถึง สิทธิทางกฎหมายที่คุ้มครองผลงานอันเกิดจากความคิดสร้างสรรค์ของมนุษย์ เพื่อให้เจ้าของผลงานมีสิทธิในการควบคุมการใช้ประโยชน์ และการเผยแพร่ผลงานของตน โดยไม่ถูกผู้อื่นนำไปใช้โดยไม่ได้รับอนุญาต

ทรัพย์สินทางปัญญาสามารถแบ่งออกเป็นหลายประเภท ได้แก่

1. ลิขสิทธิ์ (Copyright) คุ้มครองงานเขียน งานศิลปะ ดนตรี ภาพยนตร์ และโปรแกรมคอมพิวเตอร์
2. สิทธิบัตร (Patent) คุ้มครองการประดิษฐ์คิดค้นและนวัตกรรม
3. เครื่องหมายการค้า (Trademark) คุ้มครองชื่อ สัญลักษณ์ หรือเครื่องหมายที่ใช้ทางการค้า
4. ความลับทางการค้า (Trade Secret) คุ้มครองข้อมูลทางธุรกิจที่มีคุณค่า

การเคารพสิทธิในทรัพย์สินทางปัญญาเป็นสิ่งสำคัญ เนื่องจากช่วยส่งเสริมการสร้างสรรค์ผลงานใหม่ ๆ และสร้างความเป็นธรรมแก่เจ้าของผลงาน ผู้ใช้ควรใช้ผลงานของผู้อื่นอย่างถูกต้องตามกฎหมาย เช่น ขออนุญาตหรืออ้างอิงแหล่งที่มา และไม่ละเมิดสิทธิของผู้อื่น

ข้อละเว้นการละเมิดลิขสิทธิ์

1. การใช้โดยสุจริต (Fair Use) ต้องเป็นการใช้โดยไม่มีเจตนาแสวงหากำไร และไม่เอาเปรียบเจ้าของลิขสิทธิ์
2. ไม่กระทบต่อสิทธิของเจ้าของผลงาน การใช้งานต้องไม่ทำให้เจ้าของลิขสิทธิ์เสียประโยชน์ทางเศรษฐกิจอย่างไม่เป็นธรรม
3. ใช้เท่าที่จำเป็น ใช้เพียงบางส่วนของผลงาน ไม่ใช่นำผลงานทั้งหมดมาใช้โดยไม่จำเป็น
4. มีวัตถุประสงค์เพื่อประโยชน์สาธารณะ เช่น เพื่อการศึกษา วิจัย วิจารณ์ ติชม หรือรายงานข่าว
5. ต้องอ้างอิงแหล่งที่มา แสดงความเคารพต่อเจ้าของผลงานและป้องกันการเข้าใจผิดว่าเป็นผลงานของตนเอง
6. ไม่ขัดต่อศีลธรรมและกฎหมายอื่น การใช้ผลงานต้องไม่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

หลักการพิจารณาการใช้งานลิขสิทธิ์

การใช้งานลิขสิทธิ์เป็นสิ่งที่ต้องพิจารณาอย่างรอบคอบ เพื่อให้การนำผลงานของผู้อื่นมาใช้เป็นไปอย่างถูกต้องตามกฎหมาย และไม่ละเมิดสิทธิของเจ้าของผลงาน หลักการพิจารณาการใช้งานลิขสิทธิ์มีแนวทางสำคัญดังต่อไปนี้

วัตถุประสงค์ของการใช้งาน พิจารณาว่าเป็นการใช้เพื่อการศึกษา วิจัย วิจารณ์ หรือเพื่อแสวงหากำไร หากเป็นเชิงพาณิชย์จะมีความเสี่ยงในการละเมิดสูงกว่า

1. **ลักษณะของผลงาน** ผลงานที่มีความคิดสร้างสรรค์สูง เช่น งานดนตรีหรือภาพยนตร์ จะได้รับการคุ้มครองมากกว่าข้อมูลทั่วไป
2. **ปริมาณและส่วนสำคัญของผลงานที่นำมาใช้** การใช้เพียงบางส่วนที่จำเป็นมีความเหมาะสมมากกว่าการใช้ผลงานทั้งหมดหรือส่วนที่เป็นหัวใจสำคัญของผลงาน
3. **ผลกระทบต่อเจ้าของลิขสิทธิ์** ต้องไม่กระทบต่อรายได้ โอกาสทางการค้า หรือสิทธิของเจ้าของผลงานอย่างไม่เป็นธรรม

4. **การอ้างอิงแหล่งที่มา** ควรระบุชื่อผู้สร้างสรรค์และแหล่งที่มาของผลงานทุกครั้ง เพื่อแสดงความเคารพต่อเจ้าของผลงาน
5. **การใช้โดยสุจริต**
   ต้องไม่มีเจตนาละเมิดหรือเอาเปรียบ และใช้ผลงานอย่างเหมาะสมตามขอบเขตที่กฎหมายกำหนด

เบราว์เซอร์และความเป็นส่วนตัว

เบราว์เซอร์ (Browser) คือ โปรแกรมที่ใช้สำหรับเข้าถึงเว็บไซต์บนอินเทอร์เน็ต เช่น Google Chrome, Microsoft Edge, Mozilla Firefox และ Safari เบราว์เซอร์ทำหน้าที่แสดงผลข้อมูลจากเว็บไซต์ และเป็นเครื่องมือสำคัญที่ผู้ใช้ใช้งานอินเทอร์เน็ตในชีวิตประจำวัน

ความเป็นส่วนตัว (Privacy) เป็นสิ่งสำคัญในการใช้งานเบราว์เซอร์ เนื่องจากการท่องเว็บไซต์อาจมีการเก็บข้อมูลของผู้ใช้ เช่น ประวัติการเข้าชมเว็บไซต์ คุกกี้ รหัสผ่าน และข้อมูลส่วนบุคคล หากไม่มีการป้องกันที่เหมาะสม อาจทำให้ข้อมูลรั่วไหลหรือถูกนำไปใช้โดยไม่ได้รับอนุญาต

เบราว์เซอร์ในปัจจุบันมีเครื่องมือช่วยปกป้องความเป็นส่วนตัว เช่น โหมดไม่ระบุตัวตน (Incognito/Private Mode) การตั้งค่าควบคุมคุกกี้ การบล็อกตัวติดตาม (Tracking) และการล้างประวัติการใช้งาน ผู้ใช้ควรตั้งค่าความเป็นส่วนตัวให้เหมาะสม และหลีกเลี่ยงการเข้าสู่เว็บไซต์ที่ไม่น่าเชื่อถือ

การเข้าถึงสื่อดิจิทัล

สื่อดิจิทัล หมายถึง สื่อหรือข้อมูลที่ถูกสร้าง จัดเก็บ และเผยแพร่ในรูปแบบดิจิทัล โดยใช้เทคโนโลยีคอมพิวเตอร์และอินเทอร์เน็ตในการเข้าถึงและรับชม

ตัวอย่างของสื่อดิจิทัล ได้แก่

- เว็บไซต์
- สื่อสังคมออนไลน์ เช่น Facebook, YouTube, TikTok
- วิดีโอและภาพดิจิทัล
- หนังสืออิเล็กทรอนิกส์ (E-book)
- เพลงและเสียงดิจิทัล
- แอปพลิเคชันต่าง ๆ

สื่อดิจิทัลมีจุดเด่นคือ สามารถเข้าถึงได้ง่าย รวดเร็ว แก้ไขและเผยแพร่ได้สะดวก และมีการโต้ตอบกับผู้ใช้งานได้ ทำให้มีบทบาทสำคัญในด้านการศึกษา การสื่อสาร และการดำเนินชีวิตประจำวัน

การเข้าถึงสื่อดิจิทัล

การเข้าถึงสื่อดิจิทัล หมายถึง ความสามารถของบุคคลในการเข้าถึง ใช้งาน และรับข้อมูลข่าวสารจากสื่อในรูปแบบดิจิทัล เช่น เว็บไซต์ สื่อสังคมออนไลน์ วิดีโอออนไลน์ หนังสืออิเล็กทรอนิกส์ และแอปพลิเคชันต่าง ๆ ผ่านอุปกรณ์ดิจิทัล เช่น คอมพิวเตอร์ สมาร์ตโฟน และแท็บเล็ต ในปัจจุบัน สื่อดิจิทัลมีบทบาทสำคัญต่อการศึกษา การสื่อสาร และการเรียนรู้ตลอดชีวิต การเข้าถึงสื่อดิจิทัลอย่างทั่วถึงช่วยลดช่องว่างทางดิจิทัล ทำให้ประชาชนสามารถเข้าถึงข้อมูลและความรู้ได้อย่างเท่าเทียม อย่างไรก็ตาม ผู้ใช้งานจำเป็นต้องมีทักษะในการคัดกรองข้อมูล เพื่อหลีกเลี่ยงข้อมูลเท็จและสื่อที่ไม่เหมาะสม นอกจากนี้ การเข้าถึงสื่อดิจิทัลควรคำนึงถึงสิทธิและความปลอดภัย เช่น การเคารพลิขสิทธิ์ ความเป็นส่วนตัว และการใช้สื่ออย่างมีจริยธรรม เพื่อให้การใช้สื่อดิจิทัลเกิดประโยชน์สูงสุดต่อทั้งตนเองและสังคม

ประเภทของสื่อดิจิทัล

สื่อดิจิทัลสามารถแบ่งออกเป็นหลายประเภทตามลักษณะการนำเสนอและการใช้งาน ดังนี้

1. **สื่อข้อความ (Text)** เช่น เว็บไซต์ บทความ ข่าวออนไลน์ และเอกสารอิเล็กทรอนิกส์
2. **สื่อภาพ (Image)** เช่น ภาพถ่ายดิจิทัล อินโฟกราฟิก และภาพกราฟิกต่าง ๆ
3. **สื่อเสียง (Audio)** เช่น เพลงดิจิทัล พอดแคสต์ และไฟล์เสียงออนไลน์
4. **สื่อวิดีโอ (Video)** เช่น วิดีโอออนไลน์ ภาพยนตร์ดิจิทัล และคลิปวิดีโอต่าง ๆ
5. **สื่อมัลติมีเดีย (Multimedia)** เป็นการผสมผสานข้อความ ภาพ เสียง และวิดีโอเข้าด้วยกัน เช่น สื่อการเรียนออนไลน์
6. **สื่อสังคมออนไลน์ (Social Media)** เช่น Facebook, Instagram, YouTube, TikTok ใช้สำหรับการสื่อสารและแบ่งปันข้อมูล
7. **สื่อโต้ตอบ (Interactive Media)** เช่น เกมออนไลน์ แอปพลิเคชัน และเว็บไซต์ที่ผู้ใช้มีส่วนร่วม

ประเภทการเข้าถึงอินเทอร์เน็ต

การเข้าถึงอินเทอร์เน็ตสามารถแบ่งออกเป็นหลายประเภท ตามเทคโนโลยีและรูปแบบการเชื่อมต่อ ดังนี้

1. การเชื่อมต่อผ่านสายโทรศัพท์ (Dial-up) เป็นการเชื่อมต่อแบบดั้งเดิม ความเร็วต่ำ ใช้สายโทรศัพท์บ้าน
2. การเชื่อมต่อแบบ ADSL / DSL ใช้สายโทรศัพท์ แต่มีความเร็วสูงกว่า Dial-up เหมาะสำหรับบ้านและสำนักงาน
3. การเชื่อมต่อผ่านสายเคเบิล (Cable Internet) ใช้สายเคเบิลทีวี มีความเร็วสูงและเสถียร
4. การเชื่อมต่อผ่านใยแก้วนำแสง (Fiber Optic) มีความเร็วสูงมาก เหมาะสำหรับการใช้งานอินเทอร์เน็ตความเร็วสูง
5. การเชื่อมต่อผ่านเครือข่ายไร้สาย (Wi-Fi) เชื่อมต่อผ่านอุปกรณ์กระจายสัญญาณ เหมาะสำหรับบ้าน โรงเรียน และสถานที่สาธารณะ

6. การเชื่อมต่อผ่านเครือข่ายโทรศัพท์มือถือ (3G / 4G / 5G) ใช้งานผ่านสมาร์ตโฟนหรือซิมอินเทอร์เน็ต สะดวกและพกพาได้
7. การเชื่อมต่อผ่านดาวเทียม (**Satellite Internet**) เหมาะสำหรับพื้นที่ห่างไกลที่ไม่มีโครงข่ายภาคพื้นดิน

การค้นหาข้อมูลบนอินเทอร์เน็ต

การค้นหาข้อมูลบนอินเทอร์เน็ต คือ กระบวนการสืบค้นข้อมูล ข่าวสาร หรือความรู้จากแหล่งข้อมูลออนไลน์ โดยใช้อุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ต เช่น คอมพิวเตอร์หรือสมาร์ตโฟน ผ่านโปรแกรมเว็บเบราว์เซอร์และเครื่องมือค้นหา (Search Engine) เครื่องมือค้นหาที่นิยมใช้ เช่น Google, Bing และ Yahoo ผู้ใช้สามารถพิมพ์คำค้น (Keyword) ที่เกี่ยวข้องกับเรื่องที่ต้องการค้นหา เพื่อให้ได้ข้อมูลที่ตรงตามความต้องการมากที่สุด การค้นหาข้อมูลที่มีประสิทธิภาพควรเลือกใช้คำค้นที่เหมาะสม ตรวจสอบความน่าเชื่อถือของแหล่งข้อมูล เช่น เว็บไซต์ทางการ หน่วยงานรัฐ หรือสถาบันการศึกษา และควรเปรียบเทียบข้อมูลจากหลายแหล่งก่อนนำไปใช้

เทคนิคการค้นหาข้อมูลบนอินเทอร์เน็ต

1. ใช้คำค้น (Keyword) ให้ตรงประเด็น เลือกคำที่เกี่ยวข้องกับเรื่องที่ต้องการค้นหาโดยตรง และหลีกเลี่ยงคำกว้างเกินไป
2. ใช้เครื่องหมายอัญประกาศ (“ ”) ใช้เมื่อต้องการค้นหาคำหรือประโยคแบบตรงตัว เช่น “การใช้งาน Microsoft Word”
3. ใช้เครื่องหมายลบ (-) เพื่อไม่ให้แสดงผลคำที่ไม่ต้องการ เช่น คอมพิวเตอร์ -เกม
4. ใช้คำเชื่อม AND / OR AND ใช้เมื่อต้องการข้อมูลที่มีทุกคำ OR ใช้เมื่อต้องการคำใดคำหนึ่ง
5. เลือกแหล่งข้อมูลที่น่าเชื่อถือ เช่น เว็บไซต์หน่วยงานราชการ สถาบันการศึกษา หรือองค์กรที่เชื่อถือได้
6. ตรวจสอบความถูกต้องของข้อมูล เปรียบเทียบข้อมูลจากหลายแหล่งก่อนนำไปใช้
7. ใช้ตัวกรองการค้นหา (Filter) เช่น กำหนดช่วงเวลา ภาษา หรือประเภทไฟล์
8. ค้นหาจากไฟล์เฉพาะทาง เช่น filetype:pdf เพื่อค้นหาเอกสารรายงานหรือบทความ
9. อ่านสรุปผลการค้นหา (Snippet) เพื่อพิจารณาว่าเนื้อหาตรงกับที่ต้องการหรือไม่ก่อนคลิก
10. บันทึกแหล่งที่มา เพื่อใช้อ้างอิงและป้องกันการละเมิดลิขสิทธิ์

ความหมายของข้อเท็จจริงและข้อคิดเห็น

ข้อเท็จจริง (Fact)

ข้อเท็จจริง หมายถึง ข้อมูลหรือเหตุการณ์ที่เกิดขึ้นจริง สามารถพิสูจน์ ตรวจสอบ หรือยืนยันได้จากหลักฐานที่ชัดเจน เช่น เอกสาร สถิติ หรือแหล่งข้อมูลที่น่าเชื่อถือ ข้อเท็จจริงมักไม่ขึ้นอยู่กับความรู้สึกหรือความคิดเห็นส่วนตัว

ตัวอย่างข้อเท็จจริง

- ประเทศไทยมีกรุงเทพมหานครเป็นเมืองหลวง
- น้ำเดือดที่อุณหภูมิ 100 องศาเซลเซียส (ที่ระดับน้ำทะเล)

ข้อคิดเห็น (Opinion)

ข้อคิดเห็น หมายถึง ความคิด ความรู้สึก หรือการแสดงความคิดเห็นส่วนบุคคล ซึ่งอาจแตกต่างกันไปในแต่ละบุคคล ไม่สามารถพิสูจน์ได้อย่างชัดเจนว่าถูกหรือผิด

ตัวอย่างข้อคิดเห็น

- กรุงเทพฯ เป็นเมืองที่น่าอยู่มาก
- โทรศัพท์รุ่นนี้ใช้งานได้ดีมาก

การใช้เครือข่ายสังคมอย่างระมัดระวัง

เครือข่ายสังคมออนไลน์เป็นช่องทางการสื่อสารที่ได้รับความนิยมในปัจจุบัน เช่น Facebook, Instagram, Line และ TikTok แม้จะช่วยให้การติดต่อสื่อสารเป็นไปอย่างสะดวกและรวดเร็ว แต่หากใช้งานโดยขาดความระมัดระวัง อาจก่อให้เกิดผลเสียต่อตนเองและผู้อื่นได้ การใช้เครือข่ายสังคมอย่างระมัดระวังควรเริ่มจากการไม่เปิดเผยข้อมูลส่วนตัวมากเกินไป เช่น ที่อยู่ เบอร์โทรศัพท์ หรือรหัสผ่าน ควรตั้งค่าความเป็นส่วนตัวให้เหมาะสม และยอมรับเพื่อนหรือผู้ติดตามเฉพาะบุคคลที่รู้จักหรือเชื่อถือได้ นอกจากนี้ ผู้ใช้งานควรตรวจสอบความถูกต้องของข้อมูลก่อนแชร์ ไม่เผยแพร่ข่าวปลอมหรือเนื้อหาที่อาจสร้างความเสียหายแก่ผู้อื่น ใช้ถ้อยคำสุภาพ เคารพความคิดเห็นที่แตกต่าง และหลีกเลี่ยงการกลั่นแกล้งหรือคุกคามทางออนไลน์สรุปได้ว่า การใช้เครือข่ายสังคมอย่างระมัดระวังช่วยลดความเสี่ยงด้านความปลอดภัยและปัญหาทางสังคม ทำให้การใช้งานสื่อออนไลน์เป็นไปอย่างสร้างสรรค์และปลอดภัย

ความเข้าใจและการสื่อสารยุคดิจิทัล

ในยุคดิจิทัล เทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญต่อชีวิตประจำวันของมนุษย์ การสื่อสารไม่ได้จำกัดอยู่เพียงการพูดคุยแบบเผชิญหน้าเท่านั้น แต่ยังขยายไปสู่การสื่อสารผ่านสื่อดิจิทัล เช่น สื่อสังคมออนไลน์ แอปพลิเคชันแชต อีเมล และแพลตฟอร์มออนไลน์ต่าง ๆความเข้าใจในการสื่อสารยุคดิจิทัล หมายถึง ความสามารถในการรับสาร วิเคราะห์ และตีความข้อมูลที่ได้รับอย่างถูกต้อง รวมถึงการสื่อสารความคิดเห็นหรือข้อมูลของตนเองอย่างเหมาะสม ผู้สื่อสารควรใช้ภาษาที่สุภาพ ชัดเจน และคำนึงถึงผลกระทบที่อาจเกิดขึ้นกับผู้อื่น นอกจากนี้ การสื่อสารยุคดิจิทัลต้องอาศัยความรับผิดชอบ เช่น การไม่เผยแพร่ข้อมูลเท็จ การเคารพความเป็นส่วนตัวของผู้อื่น และการใช้สื่ออย่างมีวิจารณญาณ การเข้าใจบริบทของสื่อแต่ละประเภทช่วยลดความเข้าใจผิดและความขัดแย้งในสังคมออนไลน์

ความปลอดภัยยุคดิจิทัล

ความปลอดภัยยุคดิจิทัล หมายถึง การป้องกันข้อมูลส่วนบุคคล อุปกรณ์ และระบบคอมพิวเตอร์จากภัยคุกคามทางเทคโนโลยี เช่น ไวรัสคอมพิวเตอร์ การโจรกรรมข้อมูล การหลอกลวงออนไลน์ และการถูกแฮ็ก ในปัจจุบันเทคโนโลยีดิจิทัลเข้ามามีบทบาทในชีวิตประจำวันมากขึ้น ความปลอดภัยจึงเป็นสิ่งสำคัญที่ทุกคนต้องให้ความสำคัญ การรักษาความปลอดภัยในยุคดิจิทัลควรเริ่มจากการตั้งรหัสผ่านที่คาดเดายาก ไม่ใช้รหัสผ่านเดียวกันหลายบัญชี และไม่เปิดเผยข้อมูลส่วนตัวโดยไม่จำเป็น นอกจากนี้ควรอัปเดตระบบและโปรแกรมอย่างสม่ำเสมอ เพื่อป้องกันช่องโหว่ด้านความปลอดภัย ผู้ใช้งานควรระมัดระวังการคลิกลิงก์หรือดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ ตรวจสอบความถูกต้องของเว็บไซต์ก่อนกรอกข้อมูลส่วนตัว และใช้โปรแกรมป้องกันไวรัสเพื่อเพิ่มความปลอดภัย

รอยเท้าดิจิทัล (Digital Footprint)

รอยเท้าดิจิทัล หมายถึง ร่องรอยข้อมูลที่เกิดจากการใช้งานอินเทอร์เน็ตและเทคโนโลยีดิจิทัลของบุคคล เช่น การโพสต์ข้อความ รูปภาพ วิดีโอ การกดไลก์ แสดงความคิดเห็น การค้นหาข้อมูล หรือการสมัครใช้งานเว็บไซต์ต่าง ๆ ซึ่งข้อมูลเหล่านี้สามารถถูกบันทึกและตรวจสอบได้

รอยเท้าดิจิทัลแบ่งออกเป็น 2 ประเภท ได้แก่

1. รอยเท้าดิจิทัลแบบตั้งใจ (Active Digital Footprint) เช่น การโพสต์รูปหรือข้อความบนสื่อสังคมออนไลน์
2. รอยเท้าดิจิทัลแบบไม่ตั้งใจ (Passive Digital Footprint) เช่น ข้อมูลที่เว็บไซต์เก็บไว้จากการเข้าใช้งาน คุกกี้ หรือประวัติการค้นหา

รอยเท้าดิจิทัลอาจส่งผลกระทบต่อภาพลักษณ์ ความเป็นส่วนตัว และความปลอดภัยในอนาคต เช่น ด้านการศึกษา การทำงาน หรือความน่าเชื่อถือ ผู้ใช้งานจึงควรใช้สื่อดิจิทัลอย่างระมัดระวัง คิดก่อนโพสต์ และตั้งค่าความเป็นส่วนตัวให้เหมาะสม

การพิสูจน์ตัวตนดิจิทัล

การพิสูจน์ตัวตนดิจิทัล หมายถึง กระบวนการตรวจสอบและยืนยันว่าผู้ใช้งานระบบหรือบริการออนไลน์เป็นบุคคลที่แท้จริงตามที่อ้าง เพื่อป้องกันการเข้าถึงข้อมูลหรือระบบโดยไม่ได้รับอนุญาต ในยุคดิจิทัล การพิสูจน์ตัวตนมีความสำคัญอย่างยิ่งต่อความปลอดภัยของข้อมูลส่วนบุคคลและระบบสารสนเทศ วิธีการพิสูจน์ตัวตนดิจิทัลที่นิยมใช้ ได้แก่ การใช้รหัสผ่าน (Password) การยืนยันตัวตนด้วยรหัสครั้งเดียว (OTP) การใช้ลายนิ้วมือ การสแกนใบหน้า และการยืนยันตัวตนแบบสองขั้นตอน (Two-Factor Authentication) ซึ่งช่วยเพิ่มระดับความปลอดภัยมากขึ้น ผู้ใช้งานควรตั้งรหัสผ่านที่คาดเดายาก ไม่ใช้รหัสเดียวกันหลายบัญชี และไม่เปิดเผยข้อมูลยืนยันตัวตนให้ผู้อื่น เพื่อป้องกันการถูกแอบอ้างหรือโจรกรรมข้อมูล

การพิสูจน์ตัวตนแบบสองปัจจัย (2FA) ดิจิทัล

การพิสูจน์ตัวตนแบบสองปัจจัย (Two-Factor Authentication: 2FA) คือ วิธีการยืนยันตัวตนผู้ใช้งานโดยใช้หลักฐานยืนยันมากกว่า 1 อย่าง เพื่อเพิ่มความปลอดภัยในการเข้าสู่ระบบดิจิทัล ลดความเสี่ยงจากการถูกขโมยรหัสผ่าน

ประเภทของปัจจัยในการพิสูจน์ตัวตน

1. **สิ่งที่ผู้ใช้รู้ (Something You Know)**
   เช่น รหัสผ่าน หรือรหัส PIN
2. **สิ่งที่ผู้ใช้มี (Something You Have)**
   เช่น โทรศัพท์มือถือ รหัส OTP บัตรสมาร์ตการ์ด
3. **สิ่งที่ผู้ใช้เป็น (Something You Are)**
   เช่น ลายนิ้วมือ ใบหน้า หรือม่านตา

การพิสูจน์ตัวตนแบบ 2 ปัจจัยจะเลือกใช้ 2 ปัจจัยที่แตกต่างกัน เช่น รหัสผ่านร่วมกับรหัส OTP ที่ส่งไปยังโทรศัพท์มือถือ

ข้อดีของการใช้ 2FA

- เพิ่มความปลอดภัยในการใช้งานระบบออนไลน์
- ลดความเสี่ยงจากการถูกแฮ็กหรือขโมยข้อมูล
- ปกป้องข้อมูลส่วนบุคคลได้ดียิ่งขึ้น

การเข้ารหัสข้อมูลด้วย HTTPS

HTTPS (Hypertext Transfer Protocol Secure) คือ รูปแบบการรับ–ส่งข้อมูลบนเว็บไซต์ที่มีความปลอดภัย โดยใช้การเข้ารหัสข้อมูล เพื่อป้องกันไม่ให้ข้อมูลที่ส่งผ่านอินเทอร์เน็ตถูกดักจับ แก้ไข หรือขโมยไปใช้โดยไม่ได้รับอนุญาตเมื่อผู้ใช้งานเข้าเว็บไซต์ที่ขึ้นต้นด้วย **https://** ข้อมูลที่ส่งระหว่างเว็บเบราว์เซอร์กับเว็บไซต์ เช่น ชื่อผู้ใช้ รหัสผ่าน หรือข้อมูลส่วนตัว จะถูกเข้ารหัสก่อนส่ง ทำให้ผู้อื่นไม่สามารถอ่านหรือเข้าใจข้อมูลนั้นได้ แม้จะดักจับข้อมูลไว้ได้ก็ตาม

หลักการทำงานของ HTTPS

HTTPS ใช้เทคโนโลยีการเข้ารหัสที่เรียกว่า **SSL/TLS** โดยมีการใช้กุญแจเข้ารหัสเพื่อรักษาความลับของข้อมูล ซึ่งประกอบด้วย

- การยืนยันตัวตนของเว็บไซต์ (เว็บไซต์มีตัวตนจริง)
- การเข้ารหัสข้อมูลระหว่างผู้ใช้กับเว็บไซต์
- การป้องกันการแก้ไขข้อมูลระหว่างทาง

ประโยชน์ของการใช้ HTTPS

- เพิ่มความปลอดภัยในการใช้งานเว็บไซต์
- ป้องกันการโจรกรรมข้อมูลส่วนตัว
- สร้างความน่าเชื่อถือให้กับเว็บไซต์
- ลดความเสี่ยงจากการถูกดักฟังข้อมูล (Sniffing)

การเข้ารหัสข้อมูลด้วย WPA2

WPA2 (Wi-Fi Protected Access 2) คือ มาตรฐานความปลอดภัยสำหรับเครือข่ายไร้สาย (Wi-Fi) ที่ใช้การเข้ารหัสข้อมูลเพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต และป้องกันการดักจับข้อมูลที่ส่งผ่านเครือข่ายWPA2 ใช้ระบบการเข้ารหัสที่เรียกว่า **AES (Advanced Encryption Standard)** ซึ่งมีความปลอดภัยสูง ทำให้ข้อมูลที่รับ–ส่งผ่านเครือข่าย Wi-Fi ถูกเข้ารหัสและไม่สามารถอ่านได้หากไม่มีรหัสผ่านที่ถูกต้อง

รูปแบบของ WPA2

1. **WPA2-Personal (WPA2-PSK)**
   ใช้รหัสผ่านเดียวกันสำหรับผู้ใช้งานทุกคน เหมาะสำหรับบ้านหรือเครือข่ายขนาดเล็ก
2. **WPA2-Enterprise** ใช้ระบบยืนยันตัวตนผ่านเซิร์ฟเวอร์ (เช่น RADIUS) เหมาะสำหรับองค์กรหรือสถานศึกษา

ประโยชน์ของการใช้ WPA2

- เพิ่มความปลอดภัยในการใช้งาน Wi-Fi
- ป้องกันการแอบใช้เครือข่ายโดยไม่ได้รับอนุญาต
- ปกป้องข้อมูลส่วนตัวจากการถูกดักจับ

มัลแวร์ (Malware)

มัลแวร์ (Malware) ย่อมาจาก *Malicious Software* หมายถึง โปรแกรมหรือซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อสร้างความเสียหาย รบกวน หรือขโมยข้อมูลจากคอมพิวเตอร์ โทรศัพท์มือถือ หรือระบบเครือข่ายของผู้ใช้งานโดยไม่ได้รับอนุญาต

ประเภทของมัลแวร์

1. **ไวรัส (Virus)** แพร่กระจายโดยการแนบไปกับไฟล์หรือโปรแกรม ทำให้ระบบทำงานผิดปกติ
2. **เวิร์ม (Worm)** แพร่กระจายได้เองผ่านเครือข่าย โดยไม่ต้องอาศัยการเปิดไฟล์
3. **โทรจัน (Trojan)** แฝงตัวมากับโปรแกรมที่ดูน่าเชื่อถือ แต่แอบทำอันตราย
4. **สปายแวร์ (Spyware)** แอบเก็บข้อมูลพฤติกรรมหรือข้อมูลส่วนตัวของผู้ใช้
5. **แรนซัมแวร์ (Ransomware)** เข้ารหัสข้อมูลและเรียกค่าไถ่เพื่อปลดล็อก

ผลกระทบของมัลแวร์

- ข้อมูลสูญหายหรือถูกขโมย
- ระบบคอมพิวเตอร์ทำงานช้าหรือเสียหาย
- ละเมิดความเป็นส่วนตัวของผู้ใช้

วิธีป้องกันมัลแวร์

- ติดตั้งโปรแกรมป้องกันไวรัส
- ไม่ดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ
- อัปเดตระบบและซอฟต์แวร์สม่ำเสมอ

การหลอกลวงออนไลน์

การหลอกลวงออนไลน์ หมายถึง การกระทำของผู้ไม่หวังดีที่ใช้สื่ออินเทอร์เน็ตหรือเทคโนโลยีดิจิทัลในการหลอกลวงผู้อื่น เพื่อเอาทรัพย์สิน ข้อมูลส่วนตัว หรือผลประโยชน์ต่าง ๆ โดยวิธีการหลอกลวงมักมาในรูปแบบข้อความ โทรศัพท์ อีเมล หรือสื่อสังคมออนไลน์

รูปแบบของการหลอกลวงออนไลน์

1. หลอกให้โอนเงิน เช่น แอบอ้างเป็นเจ้าหน้าที่ธนาคาร หรือหน่วยงานรัฐ
2. ฟิชชิ่ง (Phishing) หลอกให้กรอกข้อมูลส่วนตัวหรือรหัสผ่านผ่านเว็บไซต์ปลอม
3. หลอกขายสินค้าออนไลน์ โฆษณาสินค้าราคาถูก แต่ไม่ส่งของจริง
4. หลอกรักออนไลน์ (Romance Scam) สร้างความสัมพันธ์แล้วหลอกขอเงิน
5. ลิงก์หรือแอปปลอม หลอกให้คลิกลิงก์หรือดาวน์โหลดแอปที่แฝงมัลแวร์

วิธีป้องกันการหลอกลวงออนไลน์

- ไม่ให้ข้อมูลส่วนตัวหรือรหัสผ่านกับผู้อื่น
- ตรวจสอบแหล่งที่มาและความน่าเชื่อถือก่อนเชื่อ
- ไม่คลิกลิงก์แปลกปลอมหรือข้อเสนอที่ดูดีเกินจริง
- ใช้การยืนยันตัวตนแบบสองขั้นตอน (2FA)

Mobile Security & Privacy

Mobile Security & Privacy หมายถึง การป้องกันอุปกรณ์มือถือ เช่น สมาร์ตโฟนและแท็บเล็ต รวมถึงข้อมูลส่วนบุคคลของผู้ใช้งานจากการถูกโจมตี การถูกขโมยข้อมูล หรือการละเมิดความเป็นส่วนตัว ในปัจจุบันโทรศัพท์มือถือถูกใช้ในการติดต่อสื่อสาร ทำธุรกรรม และจัดเก็บข้อมูลสำคัญจำนวนมาก จึงจำเป็นต้องให้ความสำคัญกับความปลอดภัยเป็นอย่างยิ่ง

ความเสี่ยงด้านความปลอดภัยและความเป็นส่วนตัวบนมือถือ

- การติดตั้งแอปจากแหล่งที่ไม่น่าเชื่อถือ
- มัลแวร์และแอปแฝงอันตราย
- การใช้ Wi-Fi สาธารณะโดยไม่มีการป้องกัน
- การรั่วไหลของข้อมูลส่วนตัว เช่น รูปภาพ รายชื่อผู้ติดต่อ

วิธีดูแล Mobile Security & Privacy

- ตั้งรหัสผ่าน ลายนิ้วมือ หรือสแกนใบหน้า
- ดาวน์โหลดแอปจากร้านค้าอย่างเป็นทางการเท่านั้น
- ตรวจสอบสิทธิ์การเข้าถึงของแอป (Permissions)
- อัปเดตระบบปฏิบัติการและแอปสม่ำเสมอ
- หลีกเลี่ยงการเชื่อมต่อ Wi-Fi สาธารณะโดยไม่จำเป็น

ปัญหาและอุปสรรคในการอบรม/สัมมนา/พัฒนาความรู้ฯ

-

ข้อคิดเห็นและข้อเสนอแนะ

-

ลงชื่อ.....

(ว่าที่ร.ต.พงษ์อนันต์ นามวงศ์)

นายช่างโยธาชำนาญงาน

ผู้รายงาน

วันที่ ๑๑ เดือน กุมภาพันธ์ พ.ศ. ๒๕๖๙

ลงชื่อ.....

(พลฯเบญจพล มั่นเหมาะ)

ผู้อำนวยการกลุ่มสำรวจเพื่อทำแผนที่

วันที่ ๑๑ เดือน ก.พ. พ.ศ. ๖๙

ความคิดเห็นของผู้บังคับบัญชา

(✓) ทราบ

.....

.....

ลงชื่อ.....

(นายเอนก ดีพรมกุล)

ผู้อำนวยการสำนักงานพัฒนาที่ดินเขต ๗

วันที่ 16 เดือน ก.พ. พ.ศ. 69