แผนการจัดการเรียนรู้ที่ 5

หน่วยที่ 3 ใช้อย่างปลอดภัยและชอบธรรม

เรื่อง ถูกต้องปลอดภัยและมีความรับผิดชอบ

รหัสวิชา ว..... **รายวิชา** วิทยาการคำนวณ **กลุ่มสาระการเรียนรู้** วิทยาศาสตร์
ชั้นมัธยมศึกษาปีที่ 3 ภาคเรียนที่ 2 **ปีการศึกษา** 2563 **เวลา 1 ชั่วโมง**

1. มาตรฐานการเรียนรู้/ตัวชี้วัด

สาระที่ 4 เทคโนโลยี

มาตรฐาน ว 4.2 เข้าใจและใช้แนวคิดเชิงคำนวณในการแก้ปัญหาที่พบในชีวิตจริงอย่างเป็นขั้นตอนและเป็นระบบใช้เทคโนโลยีสารสนเทศและการสื่อสารในการเรียนรู้การทำงาน และการแก้ปัญหาได้อย่างมีประสิทธิภาพ รู้เท่าทัน และมีจริยธรรม

ตัวชี้วัด

ว 4.2 ม.3/4 ใช้เทคโนโลยีสารสนเทศอย่างปลอดภัยและมีความรับผิดชอบต่อสังคม ปฏิบัติตามกฎหมายเกี่ยวกับคอมพิวเตอร์ ใช้ลิขสิทธิ์ของผู้อื่นโดยชอบธรรม

2. จุดประสงค์การเรียนรู้สู่ตัวชี้วัด

1. สามารถวิเคราะห์และประเมินสถานการณ์การใช้เทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัยได้ (K)
2. สามารถเสนอแนวทางในการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย (K)
3. ใช้เทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัย (P)
4. ตระหนักถึงความสำคัญของคุณธรรมจริยธรรมในการใช้เทคโนโลยีสารสนเทศ (A)

3. สาระสำคัญ

การใช้เทคโนโลยีให้ถูกต้อง ปลอดภัยและมีความรับผิดชอบกับตนเองและผู้อื่น เช่น การตั้งรหัสผ่านที่ปลอดภัยเพื่อเป็นการป้องกันการคุกคาม และควรปรับเปลี่ยนพฤติกรรมของตนเองในการใช้งานบนระบบ Social Network

4. สาระการเรียนรู้

ในปัจจุบันเทคโนโลยีมีบทบาทในชีวิตประจำวันของเราทุกคน เราจึงจำเป็นต้องมีความรู้ความเข้าใจในการใช้เทคโนโลยีให้ถูกต้องปลอดภัย ทั้งกับตนเองและผู้อื่น

1) ภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศและการป้องกัน
   - วิธีคุกคามทางเทคโนโลยี
   - การป้องกันภัยคุมคาม
   - การตั้งรหัสผ่าน
2) การใช้เทคโนโลยีสารสนเทศอย่างมีความรับผิดชอบ
   - แนวทางการปฏิบัติเมื่อพบเนื้อหาที่ไม่เหมาะสม
   - ผลกระทบการเผยแพร่ข้อมูลที่ไม่เหมาะสม
   - แนวทางการพิจารณาเนื้อหาก่อนการเผยแพร่ข้อมูล
   - มารยาทในการติดต่อสื่อสาร

5. กิจกรรมการเรียนรู้

ขั้นนำ (10 นาที)

5.1. ครูชี้แจงจุดประสงค์การเรียนรู้

5.2. นักเรียนทำแบบทดสอบก่อนเรียน เรื่อง ถูกต้องปลอดภัยและมีความรับผิดชอบ

5.3. ครูตั้งคำถามว่า “นักเรียนใช้เทคโนโลยีสารสนเทศเกี่ยวกับ Social Network อะไรบ้าง และใช้ทำอะไร” ครูและนักเรียนร่วมกันแสดงความคิดเห็นเกี่ยวกับพฤติกรรมการใช้เทคโนโลยีของแต่ละคน จากนั้นครูตั้งคำถามเพื่อให้นักเรียนร่วมอภิปรายว่า “การใช้งาน Social Network ในปัจจุบันมีความเสี่ยงที่จะเกิดภัยคุกคามอย่างไร”

หมายเหตุ: วีดิทัศน์ดังกล่าวเป็นเพียงแค่ตัวอย่างเท่านั้น หากครูมีสื่ออื่น ๆ หรือข่าวที่กำลังเป็นประเด็นสนใจในปัจจุบันเกี่ยวกับ พ.ร.บ.คอมพิวเตอร์ (เช่น การแสดงความคิดเห็นต่าง ๆ ในสื่อสังคมออนไลน์) สามารถยกมาพูดคุยกับนักเรียนได้เช่นเดียวกัน

ขั้นสอน (35 นาที)

5.4. นักเรียนศึกษา**ใบความรู้ เรื่อง “การใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย”**

5.5. ครูและนักเรียนร่วมอภิปรายเกี่ยวกับการตั้งรหัสผ่าน (Password) ว่ามีความสำคัญอย่างไรบ้างกับความปลอดภัยของข้อมูลในยุคปัจจุบัน

5.6. นักเรียนทำ <u>กิจกรรม ปลอดภัยใช่เลย</u> โดยนักเรียนเข้าไปตรวจสอบความปลอดภัยของรหัสผ่านของนักเรียนเองที่ https://howsecureismypassword.net (หรือเว็บไซต์อื่นๆ ที่สามารถตรวจสอบความปลอดภัยของรหัสผ่าน)

5.7. นักเรียนแต่ละคนทำ**ใบกิจกรรมเรื่อง "รู้ทัน ห่างไกลภัยคุกคาม"**

ขั้นสรุป (5 นาที)

5.8 นักเรียนทำแบบทดสอบหลังเรียนเรื่อง ถูกต้องปลอดภัยและมีความรับผิดชอบ

5.9 ครูและนักเรียนร่วมกันสรุปถึงความสำคัญในการรู้เท่าทันภัยคุกคามจากเทคโนโลยีในยุคปัจจุบัน โดยอาจเปิดวีดิทัศน์ "การป้องกันภัยคุกคามบนอินเทอร์เน็ต " ประกอบ (URL: https://www.youtube.com/watch?v=aRllUtizMcE)

6. สื่อการเรียนรู้/แหล่งเรียนรู้

6.1. วีดิทัศน์ "การป้องกันภัยคุกคามบนอินเทอร์เน็ต" (URL: https://www.youtube.com/watch?v=aRllUtizMcE)

6.2. ใบความรู้ เรื่อง "การใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย"

6.3. ใบกิจกรรมเรื่อง รู้ทัน ห่างไกลภัยคุกคาม

6.4. แบบทดสอบก่อนเรียน เรื่อง ถูกต้องปลอดภัยและมีความรับผิดชอบ

6.5. แบบทดสอบหลังเรียน เรื่อง ถูกต้องปลอดภัยและมีความรับผิดชอบ

7. การวัดและประเมินผล

ตัวชี้วัด	ชิ้นงาน / ภาระงาน	วิธีการประเมิน	เครื่องมือการประเมิน	ผู้ประเมิน	เกณฑ์ประเมิน
1. สามารถวิเคราะห์และประเมินสถานการณ์การใช้เทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัยได้ (K)	การตอบคำถาม/ใบกิจกรรม	ตรวจคำตอบ/ ใบกิจกรรม/ สังเกตและประเมินพฤติกรรม	แบบทดสอบ/แบบประเมิน/แบบสังเกตพฤติกรรม	ครู	มีระดับคุณภาพผ่าน/พอใช้ขึ้นไป
2. สามารถเสนอแนวทางในการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย (K)	การตอบคำถาม/ใบกิจกรรม	ตรวจคำตอบ/ ใบกิจกรรม/ สังเกตและประเมินพฤติกรรม	แบบทดสอบ/แบบประเมิน/แบบสังเกตพฤติกรรม	ครู	มีระดับคุณภาพผ่าน/พอใช้ขึ้นไป
3. ใช้เทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัย (P)	ใบกิจกรรม	ตรวจใบกิจกรรม	แบบประเมิน	ครู	มีระดับคุณภาพผ่าน/พอใช้ขึ้นไป
4. ตระหนักถึงความสำคัญของคุณธรรมจริยธรรมในการใช้เทคโนโลยีสารสนเทศ (A)	การตอบคำถาม/ใบกิจกรรม	สังเกตและประเมินพฤติกรรม	แบบสังเกตพฤติกรรม	ครูและนักเรียน	มีระดับคุณภาพผ่าน/พอใช้ขึ้นไป

เกณฑ์การประเมิน

รายการประเมิน	เกณฑ์ระดับคุณภาพ (คะแนน)			
	ไม่ผ่าน/ปรับปรุง (0)	พอใช้ (1)	ดี (2)	ดีเยี่ยม (3)
1. สามารถวิเคราะห์และประเมินสถานการณ์การใช้เทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัยได้ (K)	ไม่สามารถวิเคราะห์และประเมินสถานการณ์ได้/วิเคราะห์และประเมินไม่ถูกต้อง	วิเคราะห์และประเมินได้ถูกต้องว่าประเด็นใดเสี่ยงต่อภัยคุกคาม แต่ไม่ครบถ้วนและไม่ให้เหตุผลประกอบ	วิเคราะห์และประเมินได้ถูกต้อง ครบถ้วน ว่าประเด็นใดเสี่ยงต่อภัยคุกคามและให้เหตุผลประกอบได้ แต่ไม่สอดคล้องหรือไม่ครอบคลุมทุกประเด็น	วิเคราะห์และประเมินได้ถูกต้อง ครบถ้วน ว่าประเด็นใดเสี่ยงต่อภัยคุกคามและให้เหตุผลประกอบได้สอดคล้องครอบคลุมทุกประเด็น
2. สามารถเสนอแนวทางในการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย (K)	ไม่ได้เสนอแนวทางในการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย	เสนอแนวทางในการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัยได้ แต่ไม่เหมาะสม	เสนอแนวทางในการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัยได้ปลอดภัยและเหมาะสม	เสนอแนวทางในการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัยได้ปลอดภัยเหมาะสมและเป็นไปได้ในการปฏิบัติตามสถานการณ์
3. ใช้เทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัย (P)	ไม่ได้ตอบคำถามในใบกิจกรรม/ตอบคำถามได้ไม่ถูกต้อง	ตอบคำถามถูกอย่างน้อย 3 ข้อย่อย แต่ไม่ได้ให้เหตุผลประกอบ/เหตุผลไม่เหมาะสม	ตอบคำถามถูกอย่างน้อย 6 ข้อย่อย และให้เหตุผลประกอบได้แต่ไม่สอดคล้องหรือไม่ครอบคลุมทุกประเด็น	ตอบคำถามถูกทุกข้อและให้เหตุผลประกอบได้สอดคล้องครอบคลุมทุกประเด็น

รายการประเมิน	เกณฑ์ระดับคุณภาพ (คะแนน)			
	ไม่ผ่าน/ปรับปรุง (0)	พอใช้ (1)	ดี (2)	ดีเยี่ยม (3)
4. ตระหนักถึงความสำคัญของคุณธรรมจริยธรรมในการใช้เทคโนโลยีสารสนเทศ (A)	ใช้เทคโนโลยีสารสนเทศไม่เหมาะสมต้องแนะนำ กระตุ้นและควบคุมตลอดเวลา	ใช้เทคโนโลยีสารสนเทศอย่างถูกต้อง เหมาะสมแต่บางครั้งยังต้องได้รับคำแนะนำจากผู้อื่น	ใช้เทคโนโลยีสารสนเทศอย่างถูกต้อง เหมาะสม เป็นส่วนใหญ่และไม่ส่งผลกระทบ	ใช้เทคโนโลยีสารสนเทศอย่างถูกต้อง เหมาะสม เกิดประโยชน์

องค์ประกอบในการประเมิน/รายการประเมิน	น้ำหนักคะแนน	คะแนนเต็ม
1. สามารถวิเคราะห์และประเมินสถานการณ์การใช้เทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัยได้ (K)	3	9
2. สามารถเสนอแนวทางในการใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย (K)	2	6
3. ใช้เทคโนโลยีสารสนเทศอย่างถูกต้องและปลอดภัย (P)	3	9
4. ตระหนักถึงความสำคัญของคุณธรรมจริยธรรมในการใช้เทคโนโลยีสารสนเทศ (A)	2	6
รวม	10	30

เกณฑ์การให้คะแนน

พฤติกรรมที่ปฏิบัติชัดเจนและสม่ำเสมอ ให้ 3 คะแนน
พฤติกรรมที่ปฏิบัติชัดเจนและบ่อยครั้ง ให้ 2 คะแนน
พฤติกรรมที่ปฏิบัติบางครั้ง ให้ 1 คะแนน
พฤติกรรมที่ไม่ปฏิบัติ ให้ 0 คะแนน

เกณฑ์การให้คะแนนและแปลผลระดับคุณภาพ

คะแนน	ระดับคุณภาพ
27-30	ดีเยี่ยม
21-26	ดี
15-20	ผ่าน/พอใช้
0-14	ไม่ผ่าน/ปรับปรุง

สรุปผลการประเมิน

ผ่าน มีระดับคุณภาพ ผ่าน/พอใช้ขึ้นไป
ไม่ผ่าน มีระดับคุณภาพ ไม่ผ่าน/ปรับปรุง

9. บันทึกผลหลังการสอน

9.1 สรุปผลการเรียนการสอน

9.1.1 นักเรียนจำนวน .....คน

ผ่านจุดประสงค์การเรียนรู้ .....คน คิดเป็นร้อยละ.....

ไม่ผ่านจุดประสงค์การเรียนรู้ .....คน คิดเป็นร้อยละ.....

ได้แก่

1. .....(ชื่อนักเรียน).....

2. .....(ชื่อนักเรียน).....

นักเรียนที่มีความสามารถพิเศษได้แก่

1. .....(ชื่อนักเรียน).....

2. .....(ชื่อนักเรียน).....

9.2 ปัญหา/อุปสรรค

(ผลการประเมินที่ไม่เป็นไปตามจุดประสงค์สู่ตัวชี้วัด คุณลักษณะหรือสมรรถนะของผู้เรียน)

.....

.....

9.3 แนวทางแก้ไข/แนวทางการพัฒนา

(แนวทางการแก้ปัญหา/พัฒนานักเรียนให้ได้ ตามตัวชี้วัด คุณลักษณะ หรือสมรรถนะของผู้เรียน)

.....

.....

.....

ลงชื่อ.....

(.....)

ตำแหน่ง ครูวิทยฐานะ .....

ความเห็นของหัวหน้าสถานศึกษา/ผู้ที่ได้รับมอบหมาย

แผนการจัดการเรียนรู้ของ.....สรุปผล ดังนี้

1. เป็นแผนการจัดการเรียนรู้ที่

   ❒ นำไปใช้ได้จริง

   ❒ ควรปรับปรุงก่อนนำไปใช้ (ระบุ) .....

   .....

   .....

2. การจัดกิจกรรมการเรียนรู้

   ❒ มีกิจกรรมการเรียนรู้ที่หลากหลาย สอดคล้องกับศักยภาพของผู้เรียน

   ❒ เน้นการคิด

   ❒ มีการบูรณาการ

   ❒ ฝึกทักษะการปฏิบัติจริง

   ❒ มีการสร้างองค์ความรู้ด้วยตนเอง

3. ข้อเสนอแนะอื่น ๆ

   .....

   .....

   .....

ลงชื่อ.....

(.....)

ตำแหน่ง .....

ใบความรู้
เรื่อง การใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย

เทคโนโลยี (Technology) ตามพจนานุกรมราชบัณฑิตยสถาน คือ วิทยาการที่นำเอาความรู้ทางวิทยาศาสตร์มาใช้ให้เกิดประโยชน์ในทางปฏิบัติ เช่น อุตสาหกรรม เป็นต้น

สารสนเทศ (Information) ตามพจนานุกรมราชบัณฑิตยสถาน คือการแสดงหรือชี้แจงข่าวสารข้อมูลต่าง ๆ

เทคโนโลยีสารสนเทศ (IT : Information Technology) หมายถึง การนำวิทยาการที่ก้าวหน้าทางด้านคอมพิวเตอร์และ การสื่อสารมาสร้างมูลค่าเพิ่มให้กับสารสนเทศ ทำให้สารสนเทศ มีประโยชน์และใช้งานได้กว้างขวางมากขึ้น

ในปัจจุบันเทคโนโลยีมีบทบาทในชีวิตประจำวัน ของเราทุกคน เราจึงจำเป็นต้องมีความรู้ความเข้าใจ ในการใช้เทคโนโลยีให้ถูกต้องปลอดภัย ทั้งกับตนเองและผู้อื่น

<u>ภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศและการป้องกัน</u>

ปัจจุบันอินเทอร์เน็ตเข้ามามีบทบาทในการใช้ชีวิตประจำวัน ไม่ว่าจะเป็นด้านการศึกษา การดำรงชีวิต การสื่อสาร การศึกษา และอื่น ๆ อีกมากมาย เมื่อมีความสะดวกสบายมากเท่าใด ความปลอดภัยของข้อมูลที่เราจะนำเข้าในระบบยิ่งเป็นสิ่งที่สำคัญ การเผยแพร่ การนำเข้าข้อมูลต่าง ๆ ก็เช่นกัน ดังนั้นจึงมีความจำเป็นที่จะต้องเรียนรู้และทำความเข้าใจ

1. วิธีคุกคามทางเทคโนโลยี

1.1 การคุกคามโดยใช้หลักจิตวิทยา เป็นการคุกคามที่ใช้การหลอกลวงเพื่อให้ได้ข้อมูลที่ต้องการโดยไม่ต้องใช้ความชำนาญด้านไอที เช่น การใช้กลวิธีการต่าง ๆ เพื่อให้ได้รหัสผ่านหรือส่งข้อมูลที่สำคัญให้ โดยหลอกว่าจะได้รับรางวัลแต่ต้องทำตามเงื่อนไขที่กำหนด ซึ่งสิ่งที่เกิดขึ้นอาจป้องกันได้ยากเพราะเกิดจากความเชื่อใจ แต่ป้องกันได้โดยให้นักเรียนระมัดระวังในการให้ข้อมูลส่วนตัวกับบุคคลอื่น

1.2 การคุกคามด้วยเนื้อหาที่ไม่เหมาะสม ข้อมูลและเนื้อหาที่มีอยู่ในแหล่งต่างๆ บนอินเทอร์เน็ตมีเป็นจำนวนมากเพราะสามารถสร้างและเผยแพร่ได้ง่าย ทำให้ข้อมูลอาจไม่ได้รับการตรวจสอบความถูกต้องและความเหมาะสม ดังนั้นข้อมูลบางส่วนอาจก่อให้เกิดปัญหากับนักเรียนได้

แหล่งข้อมูลที่มีเนื้อหาไม่เหมาะสม ได้แก่ แหล่งข้อมูลที่เกี่ยวข้องกับความรุนแรง การยุยงให้เกิดความแตกแยก วุ่นวายในสังคม การพนัน สื่อลามกอนาจาร เนื้อหาที่เป็นการหมิ่นประมาท และการกระทำที่เกี่ยวข้องกับสิ่งที่ผิดต่อกฎหมายและจริยธรรม

1.3 การคุกคามโดยใช้โปรแกรม เป็นการคุกคามโดยใช้โปรแกรมเป็นเครื่องมือสำหรับก่อปัญหาด้านไอที โปรแกรมดังกล่าวเรียกว่า มัลแวร์ (malicious software: malware) ซึ่งมีหลายประเภท เช่น ไวรัสคอมพิวเตอร์ (Computer Virus), เวิร์ม (Worm), ม้าโทรจัน (Trojan Horse Virus) สปายแวร์ (Spyware) โปรแกรมโฆษณา (Advertising Supported Software: Adware) และ โปรแกรมเรียกค่าไถ่ (Ransomware)

สามารถศึกษาข้อมูลการคุกคามโดยใช้โปรแกรมเพิ่มเติมได้ที่วีดิทัศน์ “ภัยคุกคามทางคอมพิวเตอร์” (URL: https://www.youtube.com/watch?v=nkRjJMRSWCw)

2. การป้องกันภัยคุกคาม

การป้องกันภัยคุกคามด้านเทคโนโลยี เราสามารถทำได้โดย การตรวจสอบและยืนยันตัวตนของตัวผู้ใช้งานก่อนเริ่มใช้งาน ซึ่งมีด้วยกัน 3 รูปแบบคือ

2.1 ตรวจสอบจากสิ่งที่ผู้ใช้รู้ เช่น ชื่อผู้ใช้และรหัสผ่าน (Username & password) วิธีนี้ได้รับความนิยมสูงสุด

2.2 ตรวจสอบจากสิ่งที่ผู้ใช้มี เป็นการตรวจสอบตัวตนจากอุปกรณ์ที่ผู้ใช้งานต้องมี เช่น บัตรสมาร์ตการ์ด

2.3 ตรวจสอบจากสิ่งที่เป็นส่วนหนึ่งของผู้ใช้ เป็นการตรวจสอบข้อมูลชีวมาตร เช่น ลายนิ้วมือ ม่านตา ใบหน้า เสียง

3. การตั้งรหัสผ่าน

รหัสผ่านถือเป็นสิ่งสำคัญในยุคของเทคโนโลยี การเข้าใช้งานระบบต่าง ๆ บนอินเทอร์เน็ต จำเป็นต้องมีชื่อผู้ใช้และรหัสผ่านเพื่อเข้าใช้งาน การตั้งรหัสผ่าน จำเป็นต้องมีความปลอดภัยกับเจ้าของ เพื่อป้องกันการรั่วไหลของข้อมูล หรือ การใช้แอคเคาน์ ไปในทางที่ผิด ดังนั้นในการตั้งรหัสผ่านให้มีความปลอดภัย สามารถปฏิบัติได้ดังนี้

- บัญชีรายชื่อผู้ใช้แต่ละระบบ ควรใช้รหัสผ่านที่แตกต่างกัน โดยเฉพาะบัญชีที่ใช้เข้าถึงข้อมูลที่มีความสำคัญ เช่น รหัสผ่านที่ใช้ในการเข้าถึง ข้อมูลที่มีความสำคัญ เช่น รหัสผ่านของบัตรเอทีเอ็มหลายใบให้ใช้รหัสผ่านต่างกัน

- หลีกเลี่ยงการใช้รหัสผ่านโดยใช้วัน เดือน ปีเกิด ชื่อผู้ใช้ ชื่อจังหวัด ชื่อตัวละคร ชื่อสิ่งของต่าง ๆ ที่เกี่ยวข้อง หรือคำที่มีอยู่ในพจนานุกรม
- รหัสผ่านที่มีความยาว 10 ตัวอักษรนั้นเดายากกว่ารหัสผ่าน 8 ตัวอักษรถึง 4 พันเท่า ถ้าเดารหัสผ่าน 8 ตัวอักษรใช้เวลา 1 วัน เดารหัสผ่าน 10 ตัวอักษรก็ต้องใช้เวลา 4000 วัน เว็บไซต์ในทุกวันนี้มักจะต้องการรหัสผ่านความยาว 8 ตัวอักษรเป็นขั้นต่ำอยู่แล้ว แต่ถ้าต้องการความปลอดภัยจริง ๆ 10 ตัวอักษรจะดีกว่า
- ผสมผสานทั้งตัวเลข เครื่องหมาย ตัวอักษรใหญ่ และตัวอักษรเล็ก เมื่อเราใช้ตัวอักษรใหญ่ เล็ก ตัวเลข และเครื่องหมายต่าง ๆ ลงในรหัสผ่าน โอกาสที่จะเดารหัสผ่านถูกจะมีแค่ 1 ในหลายแสนล้าน
- ไม่บันทึกรหัสผ่านแบบอัตโนมัติบนโปรแกรม Browser โดยเฉพาะหากเครื่องคอมพิวเตอร์นั้นเป็นเครื่องที่ใช้ร่วมกับผู้อื่น
- หลีกเลี่ยงการบันทึกรหัสผ่านลงในกระดาษ รวมทั้งอุปกรณ์อิเล็กทรอนิกส์ด้วย หากจำเป็นต้องบันทึกก็ควรจัดเก็บไว้ในที่ที่ปลอดภัย
- ไม่บอกรหัสผ่านของตนเองกับผู้อื่น ไม่ว่ากรณีใด ๆ
- หมั่นเปลี่ยนเป็นประจำ อาจกระทำทุก 3 เดือน
- ออกจากระบบทุกครั้งที่เลิกใช้บริการต่าง ๆ บนอินเทอร์เน็ต

<u>การใช้เทคโนโลยีสารสนเทศอย่างมีความรับผิดชอบ</u>

1. แนวทางการปฏิบัติเมื่อพบเนื้อหาที่ไม่เหมาะสม

- ปฏิเสธการรับข้อมูล ทำได้โดยไม่เปิดดู ไม่บันทึกเก็บไว้ และไม่กดไลค์ (Like)
- ไม่ส่งต่อ ไม่แชร์ ไม่เผยแพร่ เพราะนอกจากจะทำให้ผู้อื่นเดือดร้อนกับข้อมูลที่ไม่เป็นความจริงแล้ว ยังอาจจะผิด พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งมีโทษทั้งจำทั้งปรับ
- แจ้งครู หรือ ผู้ปกครอง
- แจ้งผู้เกี่ยวข้องที่ดูแลเว็บไซต์นั้น เช่น Facebook YouTube เพื่อให้เจ้าของเว็บไซต์ ลบเนื้อหา หรือตัดสิทธิ์ (block) หรือจำกัดสิทธิ์การใช้งาน
- แจ้งเจ้าหน้าที่รัฐหรือตำรวจ เพื่อดำเนินการตามกฎหมาย

2. ผลกระทบการเผยแพร่ข้อมูลที่ไม่เหมาะสม

2.1 ด้านจิตใจ

- ต่อผู้เผยแพร่ รู้สึกผิดกับการกระทำของตนเอง หรือรู้สึกเสียใจเมื่อผู้อื่นมีพฤติกรรมเลียนแบบการกระทำที่ไม่เหมาะสม
- ต่อผู้อื่น เกิดความเสียใจ ทำให้เกิดความรู้สึกอับอาย ไม่ปลอดภัย กลัว รู้สึกไม่มั่นคง มีบาดแผลทางจิตใจ ได้รับความเกลียดชัง สูญเสียการยอมรับจากผู้อื่น

2.2 ด้านสังคม

- ต่อผู้เผยแพร่ ถูกสังคมลงโทษ ได้รับการประณาม หรือเกลียดชังจากสังคม
- ต่อผู้อื่น ได้ผลกระทบด้านการใช้ชีวิตประจำวัน ครอบครัวเดือดร้อน ถูกประณามจากสังคม

2.3 ด้านกฎหมาย

- ต่อผู้เผยแพร่ ได้รับโทษ เนื่องจากข้อมูลเหล่านั้นอาจผิดระเบียบ กฎเกณฑ์ หรือ กฎหมาย ทำให้เสียเวลา และเสียค่าใช้จ่ายจากการดำเนินคดีตามกฎหมาย

2.4 การงานและธุรกิจ

- ต่อผู้อื่น อาจถูกให้ออกจากงานเพราะบริษัทเกิดความเข้าใจผิดจากข้อมูลที่ได้รับ เสียผลประโยชน์ทางธุรกิจ เช่น ผู้แสวงหาผลประโยชน์ หรือคู่แข่งทางธุรกิจ อาจสร้างข่าวลวง โฆษณาชวนเชื่อเพื่อสร้างความเสียหายให้กับธุรกิจคู่แข่ง

3. แนวทางการพิจารณาเนื้อหาก่อนการเผยแพร่ข้อมูล

ก่อนที่จะเผยแพร่ข้อมูลลงในอินเทอร์เน็ตต้องพิจารณาสิ่งต่อไปนี้

3.1 ความเป็นส่วนตัว (privacy) ต้องทราบว่าข้อมูลนั้นเกี่ยวข้องกับใครหรือองค์กรใดบ้าง สามารถเปิดเผยต่อผู้อื่นได้หรือไม่

3.2 ความถูกต้อง (accuracy) ข้อมูลที่ใช้ต้องมีความถูกต้อง มีความน่าเชื่อถือ

3.3 ทรัพย์สินหรือความเป็นเจ้าของ ต้องรู้ว่าใครเป็นเจ้าของข้อมูล มีความสำคัญหรือมูลค่ามากน้อยเพียงใด

3.4 การเข้าถึง เป็นการกำหนดหรือระบุให้บุคคลหรือองค์กรใดที่มีสิทธิ์ในการเข้าถึง

4. มารยาทในการติดต่อสื่อสาร

4.1 มารยาทในการใช้อีเมล

- ใช้ภาษาสุภาพ ชัดเจน ตรงประเด็น เหมาะสมกับกาลเทศะหรือผู้ที่จะสื่อสารด้วย
- ใช้อักษรตัวหนาเฉพาะข้อความที่ต้องการเน้นเท่านั้น
- ระบุหัวเรื่อง ชื่อผู้ที่จะสื่อสาร และระบุตัวตนของผู้ส่งให้ชัดเจน
- ระบุชื่อ หรือตำแหน่งของผู้ที่จะสื่อสารให้ถูกต้องเหมาะสม
- ข้อความในอีเมลไม่ควรมีข้อความแสดงถึงเจตนาในทางเสื่อมเสีย ไม่ใช้ข้อความที่กำกวม แสดงถึงการตำหนิ ดูถูก ใส่ร้ายผู้อื่นให้ได้รับความเสียหาย
- ไม่ลักลอบส่งอีเมลโดยการปลอมแปลงชื่อผู้ส่งจนทำให้ผู้รับเข้าใจผิด
- ไม่ส่งต่ออีเมลลูกโซ่
- ไม่ส่งอีเมลขายสินค้า โฆษณา หรือข้อความรบกวนผู้อื่น

4.2 มารยาทในการใช้แชทและเครือข่ายสังคมออนไลน์

เครือข่ายสังคมออนไลน์ หรือ โซเชียลมีเดีย (Social Media) คือได้ว่าเป็นเครือข่ายสังคมออนไลน์ที่เชื่อมโยงคนหลายคนเข้าไว้ด้วยกันผ่านอินเตอร์เน็ต มีอิทธิพลต่อการดำเนินชีวิตของผู้คนเกือบทุก ๆ ด้าน ซึ่งเครือข่ายสังคมออนไลน์มีทั้งข้อดี ข้อเสีย ซึ่งผู้ใช้มีการเผยแพร่ข้อมูลส่วนตัวออกไป และทุกคนสามารถเข้าถึงข้อมูลของใครก็ได้ ข้อมูลของที่เผยแพร่ออกไปจะมีความเสี่ยงที่จะโดนแอบอ้างหรือขโมยความเป็นส่วนตัว หรือขโมยความเป็นตัวตนบนโลกออนไลน์และอาจเป็นอันตรายต่อตัวเรามากกว่าที่คิด ฉะนั้นเราต้องดูแลตัวเอง ป้องกันไม่ให้เราเกิดภัยเนื่องจากการแชร์ข้อมูลส่วนตัวบนโลกออนไลน์ ซึ่งมีรายละเอียดดังนี้

- ไม่ควรตั้งโปรไฟล์เป็นสาธารณะ
- ไม่ให้ข้อมูลส่วนตัวมากเกินไป ไม่ว่าจะเป็นวันเดือนปีเกิด เบอร์โทรศัพท์ ที่อยู่ บัตรประจำตัวประชาชน หรือบัตรเครดิตลงในโซเชียล ไม่ว่าจะอยู่ในรูปแบบข้อความ หรือรูปภาพ คิดให้รอบคอบก่อนโพสต์ข้อมูลใด ๆ
- คัดกรองคนที่ขอเป็นเพื่อน เราควรศึกษาดี ๆ ต้องเช็คให้ดีก่อน ว่าคนนั้นเป็นใครเป็นเพื่อนของเพื่อนจริงหรือเปล่า และแอดเราเป็นเพื่อนเพื่อวัตถุประสงค์ใด ถ้าไม่เป็นเพื่อนของเพื่อนจริงเราก็ไม่ขอรับเพื่อนดีกว่าเพราะว่าเขาอาจมีวัตถุประสงค์อื่นในการที่เข้ามาเป็นเพื่อนกับเรา
- การเช็คอินในสถานที่ต่าง ๆ เป็นการบอกว่าตอนนี้คุณอยู่ที่ไหน บางครั้งการโพสรูปของเราว่าไปเที่ยวอยู่จะกลับบ้านวันนั้นวันนี้ถ้าเป็นการแชร์กันระหว่างเพื่อนก็ไม่เป็นไร แต่ว่าถ้าคนอื่นที่ไม่ได้เป็นเพื่อนเราจริง ๆ ก็อาจจะเข้ามาประสงค์ร้ายได้

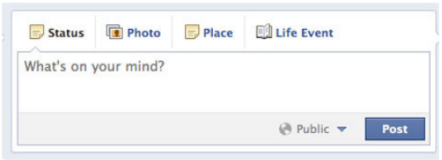
- ใช้ความระมัดระวังในการคลิกลิงก์ต่าง ๆ ที่มากับการแชร์หรือข้อความ หลีกเลี่ยงลิงก์แปลกปลอมหรือมาจากคนที่ไม่รู้จัก ซึ่งโลกออนไลน์เดี๋ยวนี้ไม่ค่อยมีการกลั่นกลองข่าวสารที่ดีพอ เพราะอาจจะไปเจอลิงก์ข่าวปลอม หรืออาจเป็นลิงก์ที่นำไปสู่ไวรัสหรือช่องทางขโมยข้อมูลของเหล่าแฮกเกอร์ได้
- ไม่ให้เบาะแสของรหัสผ่านกับคนอื่น หลายคนอยากจะแชร์ว่าหมาของเราชื่อว่าอะไร เราชอบกีฬาประเภทไหน แต่สิ่งเหล่านี้อาจจะเป็นคำถามเมื่อเราลืมรหัสผ่าน เข้าอีเมลต่าง ๆ ซึ่งถ้ามีผู้ไม่ประสงค์ดีเข้ามาคอยติดตามก็อาจจะรู้ว่าเราชอบอะไรมีสัตว์เลี้ยงตัวไหน ชอบกีฬางานอดิเรกอะไร และเขาก็สามารถเอาไปใช้เพื่อที่จะได้เอารหัสผ่านมาได้
- ไม่โพสต์รูปที่ไม่เหมาะสม เช่น โพสต์รูปตัวเองเมา หรือ โพสต์รูปตัวเองกำลังถือปืน หรือโพสต์รูปที่สื่อไปทางอนาจาร หรืออื่น ๆ เพราะสิ่งเหล่านี้อาจเป็นผลกระทบกับภาพลักษณ์ของตัวเอง
- เปิดใช้งาน Do Not Track เพื่อป้องกันการติดตามและการเก็บข้อมูลของผู้ให้บริการ ซึ่งอาจรวมไปถึงผู้ไม่หวังดีที่ลักลอบเข้ามาขโมยข้อมูลด้วย
- ใช้วิจารณญาณอย่างสูงในการรับข่าวสาร และอย่าปักใจเชื่อข้อมูลที่เผยแพร่เข้ามาในทันที รวมทั้งการกล่าวอ้างถึงแหล่งที่มาของข้อมูลนั้น ๆ เพราะอาจมีการสวมรอย หรือสมอ้างจากผู้ไม่หวังดีเพื่อสร้างข่าว หรือสร้างความเสื่อมเสียต่อแหล่งที่มานั้นได้
- ไม่โพสต์เรื่องดราม่าต่าง ๆ เป็นเรื่องเกี่ยวกับชีวิตส่วนตัว เช่น ว่าแฟนนอกใจ ทะเลาะกับเพื่อน ไม่พอใจเพื่อนร่วมงานอะไรต่าง ๆ การโพสต์แบบนี้จะเป็นการพาดพิงถึงบุคคลที่สาม อาจจะทำให้เกิด เรื่องบานปลายได้
- ยุคนี้เป็นสังคมเสรี มีอิสระทางความคิดเห็น แม้ว่าทุกคนจะมีสิทธิ์ในการแสดงความคิดเห็น แต่ทุกคำพูดและการกระทำที่ไม่เหมาะสมก็สามารถเป็นเหตุในการฟ้องร้องได้ และศาลก็อาจจะรับฟังคำร้องด้วย รวมถึงมี พ.ร.บ.ทางคอมพิวเตอร์ด้วย
- ไม่ใช้ข้อความที่เป็นชนวนก่อให้เกิดปัญหาระหว่างบุคคลและกลุ่ม
- หลีกเลี่ยงการใช้อารมณ์หรือความรู้สึกที่มากจนเกินไปทั้งในการอ่านหรือแสดงความคิดเห็น
- ไม่สวมรอยหรือแอบอ้างโดยใช้ชื่อบุคคลอื่นในการแชท แสดงความคิดเห็น หรือทำให้ผู้อื่นได้รับความเสียหาย เพราะเป็นการกระทำที่ผิดกฎหมาย
- ไม่ใช้ถ้อยคำที่ยั่วยุหรือท้าทาย เพื่อแสดงความคิดเห็น หรือความคิดเห็นที่ขัดแย้งกับผู้อื่น

คำแนะนำ
การใช้ Social Network ให้ปลอดภัย

ตั้งค่าความเป็นส่วนตัว
เพื่อกำจัดผู้สามารถเห็นโพสของเรา

ระวังเนื้อหาที่คลิกเข้าไปดู
ยินดีด้วย!!
คุณคือผู้โชคดีที่จะได้มือถือฟรี!!
คลิกที่นี่เพื่อรับของ

ไม่รับเป็นเพื่อนกับคนที่ไม่รู้จัก
เพิ่มเป็นเพื่อน

พิจารณาเนื้อหาให้ดีก่อนโพส


อย่าเปิดเผยข้อมูลส่วนตัว

ไม่ตั้ง
พาสเวิร์ดจากคำที่เรียงกันบนแป้นพิมพ์

asdfghjkl ฟหกดำสว
123456

ตั้งพาสเวิร์ดให้แข็งแรง
ประกอบด้วยอักษรตัวใหญ่ ตัวเล็ก ตัวเลข และสัญลักษณ์

sTr0NgEsT1

เปลี่ยนพาสเวิร์ดทุกๆ

6 เดือน

ห้ามใช้หรือเผยแพร่พาสเวิร์ดผู้อื่น

ไม่ควรใช้พาสเวิร์ดเดียวกันทุก Account

= password
123456

ไม่ตั้ง
พาสเวิร์ดจากบุคคลใกล้ชิดหรือคำศัพท์จากพจนานุกรม

Pass

BeeZa01
Sparzkle

<u>แหล่งอ้างอิง</u>

ธงชัย แปลกไธสง (2561). ภัยคุกคามจากเทคโนโลยี. สืบค้นเมื่อวันที่ 20 พฤศจิกายน 2562, จาก https: / / sites. google. com/ a/ sesao8 . go. th/ kruzam- computing- science/ kar- chi-thekhnoloyi-xyang-plxdphay

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี. เทคโนโลยี(วิทยาการคำนวณ) 1 . กรุงเทพฯ : ศูนย์หนังสือแห่งจุฬาลงกรณ์มหาวิทยาลัย. 2560.

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี. เทคโนโลยี(วิทยาการคำนวณ) 2 . กรุงเทพฯ : ศูนย์หนังสือแห่งจุฬาลงกรณ์มหาวิทยาลัย. 2560.

สำนักงานราชบัณฑิตสภา (2560). พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2554. สืบค้นเมื่อวันที่ 20 พฤศจิกายน 2562, จาก http://www.royin.go.th/dictionary/index.php

สำนักงานกิจการยุติธรรม (2560). กฎหมายใหม่ 36.1 : 9 ข้อระวังภัย คนใช้โซเชียล. สืบค้นเมื่อวันที่ 22 พฤศจิกายน 2562, จาก https://www.facebook.com/weareoja/photos/a.664480593637716107374182 8.533062563446187/1362978923787876/?type=3&permPage=1

A Time Design (2561). 15 ข้อควรระวัง! ในการใช้ SOCIAL MEDIA ให้ปลอดภัย รู้เท่าทัน ไม่ตกเป็นเหยื่อ. สืบค้นเมื่อวันที่ 22 พฤศจิกายน 2562, http://www.atimedesign.com/webdesign/how-to- use-social-media-safety/

ใบกิจกรรม
เรื่อง รู้ทัน ห่างไกลภัยคุกคาม

<u>คำชี้แจง</u> ให้นักเรียนพิจารณาสถานการณ์ต่อไปนี้แล้วตอบคำถามให้ครอบคลุมทุกประเด็น

สถานการณ์ที่ 1

ปกรณ์ศักดิ์ ใช้ชีวิตประจำวันส่วนใหญ่อยู่ในโลกออนไลน์ โดยใช้ Username และ Password อย่างเดียวกัน คือ 21112525 ซึ่งเป็นวันเดือนปีเกิด ในการ Log in เข้าระบบ Social Network และการทำธุรกรรมออนไลน์ บนอุปกรณ์เครื่องมือสื่อสาร และคอมพิวเตอร์โน้ตบุ๊ค โดยไม่ Log out

1.1 พฤติกรรมใดในสถานการณ์ เป็นการใช้เทคโนโลยีที่เสี่ยงต่อภัยคุกคาม เพราะเหตุใด

.....

.....

.....

.....

1.2 จากสถานการณ์ข้างต้นจะเกิดผลกระทบต่อปกรณ์ศักดิ์ ผู้อื่น และสังคมอย่างไร

.....

.....

.....

.....

1.3 จงเสนอแนวทางในการใช้เทคโนโลยีตามสถานการณ์ข้างต้นอย่างปลอดภัย

.....

.....

.....

.....

สถานการณ์ที่ 2

แหล่งอ้างอิง: http://www.thaiticketmajor.com/variety/lifestyle/11683/

2.1 พฤติกรรมใดในสถานการณ์ เป็นการใช้เทคโนโลยีที่เสี่ยงต่อภัยคุกคาม เพราะเหตุใด

.....

.....

.....

.....

2.2 จากสถานการณ์ข้างต้นจะเกิดผลกระทบต่อเจ้าของบัญชี Facebook ผู้อื่น และสังคมอย่างไร

.....

.....

.....

.....

2.3 จงเสนอแนวทางในการใช้เทคโนโลยีตามสถานการณ์ข้างต้นอย่างปลอดภัย

.....

.....

.....

.....

สถานการณ์ที่ 3

นางฟ้า (นามสมมุติ) แม่เด็กชายวัย 11 ปี ที่ใช้โทรศัพท์มือถือเล่นเกม ROV ตั้งแต่วันที่ 11 ตุลาคม 2560 จนถึงวันที่ 16 ตุลาคม 2560 โดยใช้บัตรเอทีเอ็มของแม่ซื้อไอเท็มในเกมตั้งแต่วันที่ 11-16 ต.ค. 2560 จนเงินในบัญชีธนาคารเหลืออยู่เพียง 2 บาท คาดว่าลูกชายจะใช้อีเมลของตนที่เป็นข้อมูลค้างอยู่ในเครื่องเก่านำไปกรอกสมัครเล่นเกม เพราะเกมดังกล่าวมีเงื่อนไขให้ผู้เล่นต้องมีอายุเกิน 18 ปีขึ้นไป แต่ยังไม่ทราบชัดว่าข้อมูลบัตรเอทีเอ็มที่ลูกนำไปใช้ซื้อไอเท็มต่าง ๆ ถูกนำไปเชื่อมโยงกับเกมดังกล่าวได้อย่างไร ขณะนี้กำลังปรึกษาเพื่อนและหน่วยงานต่าง ๆ ว่าจะมีทางเรียกร้องเงินกลับคืนมาได้บ้างหรือไม่ หากเรียกคืนไม่ได้ก็ต้องการให้กรณีของตนเป็นอุทาหรณ์ให้กับผู้ปกครองคนอื่น ๆ

แหล่งอ้างอิง: https://www.bangkokbiznews.com/news/detail/777705

3.1 พฤติกรรมใดในสถานการณ์ เป็นการใช้เทคโนโลยีที่เสี่ยงต่อภัยคุกคาม เพราะเหตุใด

.....

.....

.....

3.2 จากสถานการณ์ข้างต้นจะเกิดผลกระทบต่อตนเอง ผู้อื่น และสังคมอย่างไร

.....

.....

.....

3.3 จงเสนอแนวทางในการใช้เทคโนโลยีตามสถานการณ์ข้างต้นอย่างปลอดภัย

.....

.....

.....

แนวทางคำตอบใบกิจกรรม
เรื่อง รู้ทัน ห่างไกลภัยคุกคาม

<u>คำชี้แจง</u> ให้นักเรียนพิจารณาสถานการณ์ต่อไปนี้แล้วตอบคำถามให้ครอบคลุมทุกประเด็น

<u>สถานการณ์ที่ 1</u>

1.1 พฤติกรรมใดในสถานการณ์ เป็นการใช้เทคโนโลยีที่เสี่ยงต่อภัยคุกคาม เพราะเหตุใด

1. การใช้ User และ Password อย่างเดียวกัน ในการใช้ระบบ Social Network และการทำธุรกรรมออนไลน์ ซึ่งถ้าหากโดนขโมยไปหรือถูกแฮกเกอร์เข้าโจมตี ก็จะเป็นภัยต่อเรา อาจส่งผลกระทบทั้งทางร่างกาย ทรัพย์สิน และอื่น ๆ
2. ตั้งรหัสเป็น วันเดือนปี ซึ่งคาดเดาได้ง่าย ถ้ามีบุคคลอื่นที่รู้ข้อมูลในส่วนนี้
3. การไม่ Log out ระบบ ทำให้บุคคลอื่นสามารถเข้ามาดูข้อมูลส่วนตัว หรือ ทำธุรกรรมออนไลน์ หรือ ใช้ชื่อเราไปแอบอ้างในการกระทำความผิดได้

1.2 จากสถานการณ์ข้างต้นจะเกิดผลกระทบต่อปกรณ์ศักดิ์ ผู้อื่น และสังคมอย่างไร

ปกรณ์ศักดิ์จะได้รับผลกระทบดังนี้

1. ถูกค้นข้อมูลส่วนตัว ไม่ว่าจะเป็นชื่อจริง นามสกุลจริง เบอร์โทรศัพท์ เลขบัตรประชาชน รูปถ่าย และอื่น ๆ เพื่อนำไปใช้ประโยชน์ในทางที่ผิด
2. ถูกโจรกรรมข้อมูลส่วนตัว อาจนำ Facebook, line, หรือ Social media อื่น ๆ ที่เป็นของปกรณ์ศักดิ์ ไปแอบอ้างเพื่อกระทำความผิด หลอกลวงผู้อื่น
3. คนร้ายอาจขโมยรหัสผ่านบัญชี Internet Banking เพื่อขโมยเงินที่ทำให้เจ้าของบัญชีสูญเสียทรัพย์

ผู้อื่นจะได้รับผลกระทบดังนี้

1. ในกรณีที่ปกรณ์ศักดิ์ถูกโจรกรรมข้อมูล บุคคลที่เป็นเพื่อนของปกรณ์ศักดิ์อาจเป็นเหยื่อของมิจฉาชีพที่สวมรอยบัญชีเพื่อขอยืมเงินเพื่อนใน Facebook ของเจ้าของบัญชี หรือสวมรอยเอาไปทำเรื่องไม่ดี ทำให้เสื่อมเสียชื่อเสียงก็เป็นไปได้

1.3 จงเสนอแนวทางในการใช้เทคโนโลยีตามสถานการณ์ข้างต้นอย่างปลอดภัย

1 ส่วนแนวทางการตั้งรหัสผ่านที่ปลอดภัย ควรตั้งรหัสผ่านตั้งแต่ มีความยาวอย่างน้อย 8 ตัวอักษรหรือมากกว่านั้นประกอบด้วยอักขระดังต่อไปนี้อย่างน้อย 2 ใน 3

- ตัวอักษร (a-z, A-Z)
- ตัวเลข (0-9)
- เครื่องหมายหรืออักขระพิเศษ (!@#$%^&*()_+|~=\`{}[]:";'<>?,./)
-

<u>สถานการณ์ที่ 2</u>

2.1 พฤติกรรมใดในสถานการณ์ เป็นการใช้เทคโนโลยีที่เสี่ยงต่อภัยคุกคาม เพราะเหตุใด

1. การเช็คอินสถานที่ ทำให้รู้ถึงการใช้ชีวิตของเจ้าของ Facebook ว่า ณ เวลานี้ อยู่ที่ใด ทำให้รู้ความเคลื่อนไหว หรือสะกดรอยตามได้
2. การโชว์สถานะเป็นสาธารณะ ทุกคนสามารถเข้ามาดูข้อมูลใน Facebook ได้อย่างอิสระ
3. การโพสรูปตัวเองเป็นสาธารณะ ทุกคนสามารถเข้ามาดูข้อมูลใน Facebook ได้อย่างอิสระ

2.2 จากสถานการณ์ข้างต้นจะเกิดผลกระทบต่อเจ้าของบัญชี Facebook ผู้อื่น และสังคมอย่างไร

เจ้าของบัญชี Facebook จะได้รับผลกระทบดังนี้

- ผู้ร้าย หรือ มิจฉาชีพที่เข้ามาติดตามความเคลื่อนไหว ทราบข้อมูลต่างๆ ที่โพสลง Facebook ทำให้เกิดความไม่ปลอดภัยต่อตนเองและทรัพย์สิน
- อาจถูกคุกคามจากผู้ร้าย แชทข้อความลามก หรือ พฤติกรรมอนาจาร

ผู้อื่นจะได้รับผลกระทบดังนี้

- ในการถ่ายภาพและโพสภาพแบบสาธารณะ บางครั้งในภาพถ่ายมีบุคคลอื่นๆ ที่ไม่เกี่ยวข้องกับเราอยู่ในภาพ ซึ่งบุคคลเหล่านั้นอาจจะไม่ต้องการเปิดเผยการเคลื่อนไหวของตนเอง หรือในบางครั้ง Facebook ก็แท็กใบหน้าบุคคลอื่นโดยอัตโนมัติ ทำให้เป็นการละเมิดความเป็นส่วนตัวของคนอื่น**ผลกระทบต่อสังคมมีดังนี้**
- จากสถานการณ์ด้านบนเป็นการถ่ายภาพที่เห็นสถานที่กลุ่มบุคคลที่มีความสนใจในเรื่องการออกกำลังกายและเช็คอินสถานที่ ทำให้เกิดความไม่ปลอดภัยกับกลุ่มคนที่รักสุขภาพ เป็นช่องทาง หรือ เป็นข้อมูลให้กับกลุ่มมิจฉาชีพมีข้อมูลของกลุ่มเป้าหมายที่ตนเองต้องการ

2.3 จงเสนอแนวทางในการใช้เทคโนโลยีตามสถานการณ์ข้างต้นอย่างปลอดภัย

1. ตั้งค่าความเป็นส่วนตัว หลีกเลี่ยงการตั้งค่าแบบสาธารณะ อนุญาตเฉพาะเพื่อนเท่านั้น
2. ไม่ควรเช็คอินสถานที่ตลอดเวลา ทุกสถานที่ที่ไป
3. ควรตรวจสอบประวัติ หรือ คัดกรองบุคคลที่เข้ามาเป็นเพื่อนในโลกออนไลน์ เป็นต้น

<u>สถานการณ์ที่ 3</u>

3.1 พฤติกรรมใดในสถานการณ์ เป็นการใช้เทคโนโลยีที่เสี่ยงต่อภัยคุกคาม เพราะเหตุใด

1. การ Log in โดยไม่ Log out อีเมล เป็นความเสี่ยงต่อภัยคุกคามเพราะ บุคคลอื่นสามารถนำบัญชี อีเมลของเราไปทำธุรกรรม หรือ นำบัญชีเมลไปกระทำความผิดได้
2. การให้บุคคลอื่นทราบรหัสบัตรเอทีเอ็ม เป็นความเสี่ยงต่อภัยคุกคามเพราะ บุคคลอื่นสามารถใช้ทำธุรกรรมทางการเงินทำให้เราเสียทรัพย์สิน

3.2 จากสถานการณ์ข้างต้นจะเกิดผลกระทบต่อตนเอง ผู้อื่น และสังคมอย่างไร

1. นางฟ้า (นามสมมุติ) ได้รับความเดือนร้อนเรื่องทรัพย์สิน สูญเสียเงินในบัญชี
2. บุตรชายวัย 11 ปี ได้รับผลกระทบในด้าน การถูกตำหนิ ว่ากล่าวตักเตือน

3.3 จงเสนอแนวทางในการใช้เทคโนโลยีตามสถานการณ์ข้างต้นอย่างปลอดภัย

1. การใช้งานในระบบ Social Network ไม่ว่าจะเป็นการเข้า Log in ระบบใดๆ ก็ตาม โดยเฉพาะการทำธุรกรรมทางการเงิน ควร Log out เสมอ โดยเฉพาะการทำในโทรศัพท์มือถือ เพราะมีการจดจำรหัส
2. ไม่ควรบอก User และ Password กับบุคคลอื่น เพื่อเป็นการป้องกันการนำ User และ Password ของเราไปใช้ในทางไม่ถูกต้อง
3. ในกรณีเด็กผู้ปกครองต้องให้การดูแล และแนะนำให้ความรู้กับเด็กอย่างใกล้ชิด

แบบทดสอบ การใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย

1. ข้อใดเขียนคำว่า เทคโนโลยีสารสนเทศ ได้ถูกต้อง?

ก. Techno Information
ข. Information Techno
ค. Technology Information
ง. Information Technology

ตอบ ง. Information Technology

2. นักเรียนมีวิธีป้องกันการเข้าถึงข้อมูลจากผู้อื่นอย่างไร?

ก. ติดตั้งโปรแกรมสแกนไวรัส
ข. ปิดคอมพิวเตอร์ทุกครั้งหลังเลิกใช้งาน
ค. ตั้งรหัสผ่านโดยใช้วัน เดือน ปีเกิด
ง. ตั้งรหัสผ่านที่ยากต่อการคาดเดา

ตอบ ง. ตั้งรหัสผ่านที่ยากต่อการคาดเดา

3. ข้อใดคือการป้องกันตนเองจากปัญหาอาชญากรรมทางอินเทอร์เน็ต?

ก. ปิดไฟทุกครั้งหลังเลิกใช้งาน
ข. ตั้งรหัสผ่านเข้าสู่คอมพิวเตอร์
ค. ติดตั้งโปรแกรมสแกนไวรัส
ง. พิมพ์เลขบัตรประชาชนลงใน Facebook

ตอบ ข. ตั้งรหัสผ่านเข้าสู่คอมพิวเตอร์

4. ถ้านักเรียนพบว่ามีคนลืมออกจากระบบเฟซบุ๊ก นักเรียนควรปฏิบัติอย่างไร?

ก. กดออกจากระบบให้
ข. โพสต์ข้อความตามใจตนเอง
ค. ไม่สนใจ ปล่อยให้อยู่ในระบบเฟซบุ๊กต่อไป
ง. โพสต์ว่า “เจ้าของเฟซบุ๊กลืมออกจากระบบ กรุณาตรวจสอบด้วย”

ตอบ ก. กดออกจากระบบให้

5. ใครคือ “พลเมืองดิจิทัล”?

ก. สุดาเล่นเฟสบุ๊คเป็นประจำ
ข. มาลีดู youtube ทุกวัน
ค. แก้วมีความสามารถในการใช้เทคโนโลยี และสื่อดิจิทัลเป็นประจำได้อย่างปลอดภัย
ง. กล้ามีความสามารถในการใช้คอมพิวเตอร์ในสร้างแชร์เพจต่าง ๆ ได้

ตอบ ค. แก้วมีความสามารถในการใช้เทคโนโลยี และสื่อดิจิทัลเป็นประจำได้อย่างปลอดภัย

6. บุคคลใดไม่มีมารยาทในการติดต่อสื่อสารผ่านอินเทอร์เน็ต?

ก. กบตรวจสอบข้อมูลให้ถูกต้องก่อนส่งให้ผู้อื่น
ข. กล้าใช้ศัพท์สแลงในการสื่อสาร
ค. แก้วไม่เผยแพร่ข้อมูลส่วนตัวของผู้อื่น
ง. กิ๊กใช้ข้อความที่สั้น กะทัดรัด และเข้าใจง่าย

ตอบ ข. กล้าใช้ศัพท์สแลงในการสื่อสาร

7. บุคคลใดเป็นอาชญากรรมทางอินเทอร์เน็ต?

ก. นีโน่เผยแพร่วีดีโอการทำอาหารลงอินเทอร์เน็ต

ข. แนนถ่ายรูปเพื่อนแล้วส่งต่อไปยังคนอื่นโดยได้รับอนุญาต

ค. นัทใช้คอมพิวเตอร์ของเพื่อนเพื่อสืบค้นข้อมูลในอินเทอร์เน็ต

ง. นิ่มคัดลอกผลงานของเพื่อนและนำไปส่งครู

ตอบ ง. นิ่มคัดลอกผลงานของเพื่อนและนำไปส่งครู

8. ข้อใดเป็นข้อควรปฏิบัติในการใช้เทคโนโลยี?

ก. เข้าถึงข้อมูลส่วนตัวของผู้อื่น

ข. นำข้อมูลของผู้อื่นมาเผยแพร่

ค. ใช้ภาษาที่สุภาพในการติดต่อสื่อสาร

ง. ตั้งรหัสผ่าน โดยใช้วัน เดือน ปีเกิดของตนเอง

ตอบ ค. ใช้ภาษาที่สุภาพในการติดต่อสื่อสาร

9. ข้อใดเป็นพฤติกรรมที่ไม่เหมาะสมในการใช้งานอินเทอร์เน็ต?

ก. การดาวน์โหลดฟรีแวร์

ข. การอัปโหลดข่าวการเมือง

ค. การรับส่งอีเมล์

ง. การโพสต์ข้อมูลเท็จ

ตอบ ง. การโพสต์ข้อมูลเท็จ

10. พลเมืองดิจิทัลจะต้องมีความรับผิดชอบด้านใดบ้าง?

ก. ความรับผิดชอบต่อตนเอง

ข. ความรับผิดชอบต่อครอบครัวและเพื่อน

ค. ความรับผิดชอบต่อชุมชน

ง. ถูกทุกข้อ

ตอบ ง. ถูกทุกข้อ