

สรุปบทเรียน e-learning สำนักงาน กพ. (OCSC Learning Space)

หลักสูตร “วัยใส ฉลาดรู้เน็ต”

โดย นายอัศวิน เนตรนอมศักดิ์

จุดประสงค์

วิชา วัยใส ฉลาดรู้เน็ต จัดทำขึ้น เพื่อสื่อสารกับคนทุกกลุ่มทุกวัยอย่างเข้าใจง่าย โดยเฉพาะกลุ่มเยาวชนที่ถือว่าเป็นกลุ่มที่มีความเสี่ยงในลำดับต้นๆ โดยนำเอาหลักความฉลาดทางดิจิทัล ที่ส่งเสริมทักษะการเข้าสู่สังคมที่จำเป็นต่อการใช้ชีวิตในโลกออนไลน์มาเป็นแกนหลักในการอธิบายเนื้อหาพร้อมยกระดับความคิดสร้างสรรค์ทางดิจิทัล เพิ่มความรู้และความสามารถในการใช้เทคโนโลยี เครื่องมือดิจิทัลต่าง ๆ เกิดความตระหนักรู้เกี่ยวกับการใช้เทคโนโลยีดิจิทัลและอินเทอร์เน็ตอย่างมั่นคงปลอดภัย เพื่อสามารถเป็นแบบอย่างต่อสังคมได้ ซึ่งจะช่วยลดปัญหาความเสี่ยงจากการใช้อินเทอร์เน็ต และการตกเป็นเหยื่อในโลกออนไลน์

รู้ไว้ไม่ตกเทรนด์

ความฉลาดทางดิจิทัล (DQ) เป็นผลจากการศึกษาและพัฒนาของหน่วยงานที่มีชื่อเรียกว่า DQ Institute เกิดจากความร่วมมือกันของภาครัฐและเอกชนทั่วโลกประสานงานร่วมกับ World Economic Forum ที่ส่งเสริมให้เด็ก ๆ ทั่วโลกมีความรู้และทักษะในการใช้ชีวิต บนโลกออนไลน์อย่างปลอดภัย แต่ไม่ใช่แค่เด็ก ๆ เท่านั้นที่ควรเป็น “ผู้ฉลาดรู้เน็ต” แต่รวมไปถึง คุณปู่ คุณย่า และทุกคนที่ใช้งานอินเทอร์เน็ต โดยการเป็นพลเมืองดิจิทัลต้องเข้าใจและวางตัวให้เหมาะสมในการเป็นสมาชิกสังคมออนไลน์ ซึ่งมีทักษะง่าย ๆ 8 ข้อ คือ

1. ทักษะในการเป็นตัวเองที่ดี (Digital Citizen Identity) ใช้สื่อดิจิทัลสร้างภาพลักษณ์ในโลกออนไลน์ของตนเองในแง่บวกทั้งความคิด ความรู้สึก มีวิจารณญาณในการรับส่งข่าวสารและแสดงความคิดเห็นมีความเห็นอกเห็นใจผู้ร่วมใช้งานในสังคมออนไลน์ และรับผิดชอบ รู้กฎหมายและจริยธรรมในโลกออนไลน์ เช่น การละเมิดลิขสิทธิ์ การกระทำความผิด หรือการใช้คำที่สร้างความเกลียดชังผู้อื่นทางสื่อออนไลน์

2. ทักษะในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Management) ป้องกันการขโมยข้อมูล ไปสวมรอยทำธุรกรรมออนไลน์ รักษา ป้องกันความเสียหายของข้อมูล ระบบ และอุปกรณ์

3. ทักษะการคิดวิเคราะห์ มีวิจารณญาณที่ดี (Critical Thinking) สามารถวิเคราะห์แยกแยะระหว่างข้อมูลที่ถูกต้องและข้อมูลที่ผิด รู้เท่าทันสื่อและเทคโนโลยีดิจิทัล สามารถวิเคราะห์และประเมิน ข้อมูลจากแหล่งข้อมูลที่หลากหลายได้ เข้าใจรูปแบบการหลอกลวงต่าง ๆ ในโลกไซเบอร์ เช่น ข่าวปลอม เว็บบลอม ภาพตัดต่อ

4. ทักษะในการรักษาข้อมูลส่วนตัว (Privacy Management) รู้จักปกป้องข้อมูลความเป็นส่วนตัวในโลกออนไลน์ รู้เท่าทันภัยคุกคามทางอินเทอร์เน็ต เช่น มัลแวร์ ไวรัสคอมพิวเตอร์ และกลลวงทางไซเบอร์ที่ขโมยข้อมูลไปใช้ในทางที่เสียหาย

5. ทักษะในการจัดสรรเวลาหน้าจอ (Screen Time Management) บริหารเวลาที่ใช้อุปกรณ์ยุคดิจิทัล ควบคุมเพื่อให้เกิดสมดุลระหว่างโลกออนไลน์ และโลกภายนอก ตระหนักถึงอันตรายจากการใช้เวลาหน้าจอมากเกินไป การทำงานหลายอย่างในเวลาเดียวกัน และผลเสียของการเสพติดสื่อดิจิทัล

6. ทักษะในการบริหารจัดการข้อมูลที่ใช้ใช้งาน มีการทิ้งไว้บนโลกออนไลน์ (Digital Footprints) สามารถเข้าใจธรรมชาติของการใช้ชีวิตในโลกดิจิทัลว่าจะหลงเหลือร่องรอยข้อมูลทิ้งไว้เสมอเข้าใจผลลัพธ์ที่อาจเกิดขึ้นเพื่อการดูแลสิ่งเหล่านี้อย่างรับผิดชอบ

7. ทักษะในการรับมือกับการกระรณทางไซเบอร์ (Cyberbullying Management) ปิดกั้นผู้ที่กระรณและ ไม่ตอบโต้ด้วยวิธีเดียวกัน ขอความช่วยเหลือผู้ปกครอง ครู หรือผู้เชี่ยวชาญ รวมทั้งแจ้งต่อผู้ดูแลระบบเข้มแข็งและ กล้าเผชิญกับสิ่งที่เกิดขึ้นไปแล้ว

8. ทักษะการใช้เทคโนโลยีอย่างมีจริยธรรม (Digital Empathy) มีความเห็นอกเห็นใจ และสร้างความสัมพันธ์ที่ดีกับผู้อื่นบนโลกออนไลน์

เพราะโลกกว้าง อินเทอร์เน็ตจึงสำคัญ

อินเทอร์เน็ตเป็นการเชื่อมโยงอุปกรณ์คอมพิวเตอร์เข้าด้วยกันเป็นเครือข่ายขนาดใหญ่ผู้ใช้สามารถท่องเว็บไซต์ ดูวิดีโอ เล่นโซเชียลเน็ตเวิร์ก แชต วิดีโอคอล ได้อย่างสะดวก การเชื่อมต่อก็มีทั้งแบบใช้สายและแบบไร้สาย ซึ่งคอมพิวเตอร์เหล่านั้นต้องมีอุปกรณ์รับส่งสัญญาณที่สามารถรับส่งข้อมูลที่ต้องการผ่านเครือข่าย อินเทอร์เน็ตได้หากจะให้อธิบายอย่างเข้าใจง่ายมันคือเครือข่ายขนาดใหญ่ที่มีผู้ใช้งานอยู่ทั่วโลกเราอาจจะจินตนาการว่ามันเป็นเหมือนใยแมงมุมขนาดใหญ่ที่มีใยเชื่อมโยงครอบคลุมถึงกันทั้งหมดไม่ว่าใครจะอยู่ที่ไหนมุมใด ในโลกก็สามารถติดต่อกันได้

Cyberbullying ไม่ใช่เรื่องตลก

"Cyberbullying" หรือ "การกระรณทางไซเบอร์" เป็นคำที่เราคงเคยได้ยินหรืออาจจะเคยเผลอทำลงไปโดยไม่รู้ตัวเป็นการกระรณโดยใช้สื่อออนไลน์เป็นเครื่องมือเพื่อทำให้ผู้อื่นเดือดร้อนรำคาญ หรือรู้สึกไม่ดีต่าง ๆ พฤติกรรมอะไรบางอย่างที่เป็น Cyberbullying เช่น การโพสต์ภาพตัดต่อล้อเลียนหรือภาพที่ทำให้เกิดความเสียหาย การใช้ถ้อยคำนินทา ด่าทอ ให้เพื่อน ๆ รู้สึกเสียหาย อับอาย ใสร้าย ข่มขู่หรือทำให้ไม่รู้สึกไม่ปลอดภัย สวมรอยออนไลน์

ภัยออนไลน์ ร้าย แต่ป้องกันได้

10 คำแนะนำป้องกัน

อันตรายทาง Email

ไวรัสโทรจันหรือโทรจันคอมพิวเตอร์

1

ตั้ง Password ที่คาดเดาได้ยาก และเปลี่ยนบ่อยๆ

2

ดูแลช่องทางการใช้ในการ Reset รหัสผ่าน ให้ความมั่นใจคงปลอดภัย เช่น อีเมลสำรองสำหรับกู้คืนบัญชี

3

ตรวจสอบประวัติการใช้งานที่น่าสงสัย รวมทั้งช่องทางการยืนยันตัวตน อย่างสม่ำเสมอ

4

ติดตั้งโปรแกรมแอนติไวรัส อัปเดตระบบปฏิบัติการบนเบราว์เซอร์ และซอฟต์แวร์รักษาความปลอดภัย

5

หลีกเลี่ยงการใช้อีเมลผ่านเครื่องคอมพิวเตอร์สาธารณะ และไม่ควรตั้งค่าให้จำรหัสผ่าน

59

รู้ทันภัยไซเบอร์... ทำธุรกรรมออนไลน์ อย่างไรให้หายห่วง

24 ชม. ในชีวิตออนไลน์ 1,440 นาที อาจตกเป็นเหยื่อภัยร้ายในโลกไซเบอร์ 86,400 วินาที ที่สามารถป้องกันได้ถ้ารู้วิธี

1

จำกัดวงเงินทำธุรกรรมออนไลน์

2

ระวังอีเมลไซด์ประเภทฟิชซิง

3

ใช้รหัสลับแบบ

4

โดยเฉพาะธนาคารออนไลน์

5

โทรศัพท์มือถือเป็นเจ้าหน้าที่ยืนยันธุรกรรม

64

10 คำแนะนำป้องกัน

อันตรายทาง Email

ไวรัสโทรจันหรือโทรจันคอมพิวเตอร์

6

ระมัดระวังอีเมลที่มีไฟล์แนบ หรือลิงก์พาไปเว็บไซต์อื่น

7

เปลี่ยนอีเมลจากผู้ส่งที่อาจจะเป็นคนร้าย เปลี่ยนเบอร์โทรศัพท์ หากไม่แน่ใจ ควรยืนยันผ่านช่องทางอื่นที่ไม่ใช่อีเมล

8

เปิดการใช้งานยืนยันตัวตนแบบ 2 Factor Authentication

9

เมื่อได้รับอีเมลที่สงสัยให้กดปุ่ม Reply หรือ Reply All ทุกครั้ง

10

อย่าหลงเชื่ออีเมลที่หลอกให้เปลี่ยน Password หรือให้ส่งข้อมูลส่วนตัว

60

เว็บไซต์ที่ใช้บริการ ต้องมีการเข้ารหัสเสมอ

สององค์ประกอบหลักที่จำเป็นในการเข้ารหัสคือ ใบรับรองอิเล็กทรอนิกส์ หรือ SSL Certificate เป็นใบรับรอง

3

เว็บไซต์ที่ใช้บริการ ต้องมีการเข้ารหัสเสมอ

4

ตั้งพาสเวิร์ดให้ยุ่งยากไว้ก่อน

5

อย่าหลงเชื่ออีเมลที่หลอกให้เปลี่ยน Password หรือให้ส่งข้อมูลส่วนตัว

65