

การพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์สำหรับผู้เรียนชั้นประถมศึกษา Enhancing Cybersecurity Skills for Elementary Students

ผู้แต่ง ยศวัจจน์ อภิรัตน์ระพี¹
บุญรัตน์ แผลงศรี²

Yossawat Apiratrapee¹
Boonrat Plangsorn²
fedubrp@ku.ac.th

Received : 2024-11-07

Revised : 2024-12-27

Accepted : 2025-08-28

บทคัดย่อ

การพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์สำหรับผู้เรียนระดับประถมศึกษา โดยมีวัตถุประสงค์เพื่อสร้างความตระหนักและความรู้ในการป้องกันภัยคุกคามต่าง ๆ ที่พบในโลกไซเบอร์ เช่น การกลั่นแกล้งทางไซเบอร์ การล่อลวง การโจมตีข้อมูลส่วนบุคคล และการเข้าถึงเนื้อหาที่ไม่เหมาะสม การศึกษาแบ่งออกเป็นสองส่วนหลัก ได้แก่ ส่วนที่หนึ่ง การส่งเสริมความรู้ด้านความปลอดภัยไซเบอร์ การพัฒนาความฉลาดทางดิจิทัลและความฉลาดทางอารมณ์ของผู้เรียน ซึ่งครอบคลุมทักษะสำคัญ เช่น การรักษาอัตลักษณ์ออนไลน์ การคิดวิเคราะห์ข้อมูล การจัดการข้อมูลส่วนบุคคล และการใช้เวลาหน้าจออย่างเหมาะสม ส่วนที่สอง การพัฒนาทักษะด้านความปลอดภัย โดยใช้กิจกรรมการเรียนรู้เกม Interland ได้รับการออกแบบให้ผู้เรียนสามารถฝึกฝนทักษะด้านความปลอดภัยทางไซเบอร์ผ่านการเล่นเกม ตัวอย่างเช่น การฝึกทักษะคิดก่อนแชร์ข้อมูล การตรวจสอบแหล่งที่มาของข้อมูล การตั้งค่ารหัสผ่านที่ปลอดภัย และการป้องกันตนเองจากการกลั่นแกล้งทางออนไลน์ กิจกรรมเหล่านี้ช่วยให้การเรียนรู้เรื่องความปลอดภัยทางไซเบอร์เป็นไปอย่างสนุกสนาน เข้าถึงง่าย และส่งเสริมการมีส่วนร่วมอย่างมีประสิทธิภาพ

คำสำคัญ: ความปลอดภัยทางไซเบอร์, ความฉลาดทางดิจิทัล, ความฉลาดทางอารมณ์

Abstract

The development of cybersecurity skills for elementary school students aims to raise awareness and knowledge in protecting against various cyber threats, such as cyberbullying, phishing, personal data breaches, and accessing inappropriate content. The study is divided into two main parts: the first focuses on promoting cybersecurity knowledge, digital literacy, and emotional intelligence among students. This includes key skills such as safeguarding online identity, critical thinking for data analysis, personal data management, and appropriate screen time usage. The second part involves developing practical cybersecurity skills through interactive learning activities, such as the Interland game, designed to allow students to practice skills like thinking before sharing information, verifying the source of information, setting secure passwords, and defending against online bullying. These activities make cybersecurity learning engaging, accessible, and encourage effective participation.

¹ ข้าราชการครูโรงเรียนอนุบาลเคหะบางพลี(๑๐ปี สปข.)

Teacher at Anubankhehabanplee School

² ผู้ช่วยศาสตราจารย์, ดร., คณะศึกษาศาสตร์, มหาวิทยาลัยเกษตรศาสตร์,

Asst. Prof., Dr., Faculty of Education, Kasetsart University,

Keywords: Cyber Security, Digital Intelligence, Emotional Intelligence

บทนำ

การพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์สำหรับเยาวชนได้รับความสำคัญมากขึ้น เนื่องจากโลกดิจิทัลในปัจจุบันเต็มไปด้วยภัยคุกคามต่าง ๆ เช่น การหลอกลวงข้อมูลส่วนตัว การโจมตีด้วยมัลแวร์ และการกลั่นแกล้งทางไซเบอร์ การพัฒนาทักษะเหล่านี้ตั้งแต่ระดับเยาวชนไม่เพียงช่วยให้พวกเขามีการรับรู้ถึงภัยคุกคาม แต่ยังช่วยส่งเสริมให้มีทักษะในการป้องกันและจัดการกับปัญหาที่อาจเกิดขึ้นอย่างมีประสิทธิภาพ โดยเฉพาะการสร้างทักษะในด้านการตัดสินใจเชิงวิพากษ์ (Critical Thinking) การรู้เท่าทันสื่อและข่าวสาร รวมถึงการจัดการกับข้อมูลส่วนตัวในโลกออนไลน์อย่างมีความรับผิดชอบ (กนกวรรณ, 2564)

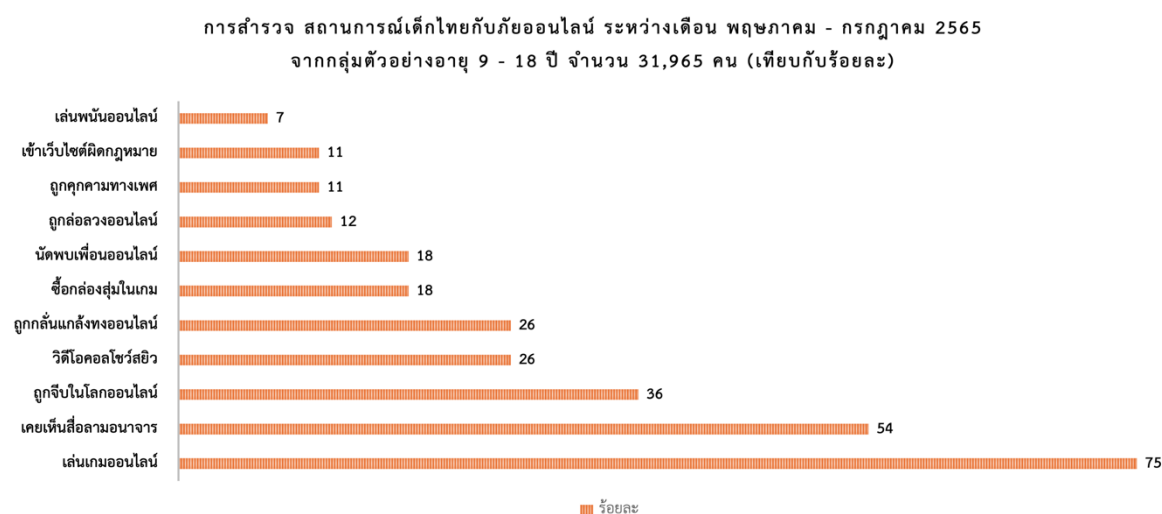
ประเทศไทยได้ให้ความสำคัญกับเรื่องดังกล่าวอย่างจริงจัง หลังจากที่รัฐบาลผลักดันนโยบายเศรษฐกิจดิจิทัล (Digital Economy) เพื่อเสริมสร้างความเข้มแข็งให้กับระบบเศรษฐกิจ โดยกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้ให้ความสำคัญและกำหนดไว้ในแผนพัฒนายุทธศาสตร์ที่ 3 ซึ่งมุ่งเน้นการสร้างสังคมคุณภาพและเท่าเทียมด้วยเทคโนโลยีดิจิทัล โดยมีเป้าหมายให้ประชาชนมีความตระหนักรู้ มีความเข้าใจ และทักษะที่จำเป็นการใช้เทคโนโลยีดิจิทัลให้เกิดประโยชน์และสร้างสรรค์ (Ministry of Digital Economy and Society, 2016 อ้างถึงใน ศุภณัฐ เพิ่มพูนวิวัฒน์ และคณะ, 2564) ทั้งนี้ ความฉลาดทางดิจิทัล หรือ DQ เป็นผลจากการศึกษาและพัฒนาของสถาบัน DQ Institute ซึ่งเป็นองค์กรความร่วมมือระหว่างภาครัฐและเอกชนทั่วโลก ดำเนินงานร่วมกับ World Economic Forum (WEF) เพื่อให้เด็ก ๆ ทั่วโลกได้รับการศึกษาเกี่ยวกับทักษะพลเมืองดิจิทัลที่มีคุณภาพและสามารถใช้ชีวิตบนโลกออนไลน์อย่างปลอดภัย ในรายงาน DQ Report 2018 ระดับทักษะความฉลาดทางดิจิทัลของเด็กไทยยังอยู่ในระดับต่ำ สำนักงานส่งเสริมเศรษฐกิจดิจิทัล กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม สำนักงานคณะกรรมการการศึกษาขั้นพื้นฐาน (สพฐ.) กระทรวงศึกษาธิการ และ DQ Institute ได้ร่วมกันดำเนินโครงการ #DQEveryChild ศึกษาเด็กไทยอายุ 8-12 ปี จำนวน 1,300 คน ผ่านการสำรวจออนไลน์ DQ Screen Time Test ร่วมกับเด็กจาก 29 ประเทศทั่วโลก จำนวนกลุ่มตัวอย่างทั้งหมด 37,967 คน พบว่า เด็กไทยมีความเสี่ยงจากภัยออนไลน์ถึงร้อยละ 60 ซึ่งสูงกว่าค่าเฉลี่ยทั่วโลกที่อยู่ร้อยละ 56 ภัยออนไลน์ที่พบได้แก่ การกลั่นแกล้งบนโลกออนไลน์ การถูกล่อลวงไปพบคนแปลกหน้า ปัญหาการติดเกม การเข้าถึงสื่อลามกอนาจาร และการพูดคุยเรื่องเพศกับคนแปลกหน้า

ดัชนีชี้วัดความปลอดภัยบนสื่อออนไลน์สำหรับเด็ก (COSI) ประจำปี 2566 พบว่าเด็กและวัยรุ่นอายุ 8-18 ปีทั่วโลกสูงเกือบ 70% ต้องเผชิญกับความเสี่ยงทางไซเบอร์อย่างน้อย 1 ครั้งในปีที่ผ่านมา สถิติที่น่าตกใจนี้แทบไม่มีการเปลี่ยนแปลงนับตั้งแต่เริ่มต้นการจัดทำดัชนีในปี 2561 โดยสถาบันตีควชานนามสถานการณ์นี้ว่าเป็น "การระบาดใหญ่ทางไซเบอร์อย่างต่อเนื่อง" ดร. ยูซยอน ปาร์ค ผู้ก่อตั้งสถาบันตีคว ระบุว่า เราได้เห็นอัตราการเสี่ยงทางไซเบอร์ในระดับสูงอย่างต่อเนื่องถึง 70% เป็นเวลา 7 ปีในเด็กและเยาวชนอายุ 8-18 ปี ตอนนี้เราเรียกปรากฏการณ์นี้ว่า "การระบาดใหญ่ทางไซเบอร์อย่างต่อเนื่อง" (Park, 2023)

ภัยอันตรายทางไซเบอร์ที่เกิดขึ้นกับผู้เรียน

กรมกิจการเด็กและเยาวชน กระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์ ได้ทำการสำรวจสถานการณ์เด็กไทยกับภัยออนไลน์ ระหว่างเดือน พฤษภาคม - กรกฎาคม 2565 จากกลุ่มตัวอย่างอายุ 9 - 18 ปี จำนวน 31,965 คน พบว่า เด็กไทยเข้าถึงสื่อโซเชียลมีเดียได้แทบทุกคน สามารถเข้าถึงสื่อลามกอนาจารได้ง่ายและมีประสบการณ์ถูกจีบในโลกออนไลน์อีกจำนวนไม่น้อย แบ่งเป็น เด็กไทย 54% เคยพบเห็นสื่อลามกอนาจาร 36% มีประสบการณ์ถูกจีบในโลกออนไลน์ ส่วนใหญ่เป็นเด็กมัธยม 26% เคยวิดีโอคอลโซวส์ยิว 26% ถูกกลั่นแกล้งรังแกทางออนไลน์ (Cyber Bullying) 12% ถูกล่อลวงออนไลน์ (Grooming) เป็นเด็กประถมอายุ 10-12 ปี และ 11% ถูกคุกคามทางเพศ นอกจากนี้ ผลสำรวจยังแสดงให้เห็นถึง พฤติกรรมการใช้งานอินเทอร์เน็ตและโซเชียลมีเดียของเด็กไทยจากกลุ่มตัวอย่างด้วย โดยระบุว่าเด็กไทย 75% เล่นเกมออนไลน์ 11% เคยเข้าเว็บไซต์ผิด

กฎหมายหรืออันตราย 7% เล่นพนันออนไลน์ 18% จ่ายเงินเพื่อซื้อกล่องสุ่มในเกม ถือเป็นรูปแบบหนึ่งของการพนัน และ 18% เคยนัดพบเพื่อนออนไลน์ (อนุกุล ปัดแก้ว, 2565)



ภาพที่ 1 กราฟแสดงการสำรวจ สถานการณ์เด็กไทยกับภัยออนไลน์

ปัจจุบันผู้เรียนมีการใช้อินเทอร์เน็ตและเทคโนโลยีดิจิทัลในชีวิตประจำวันอย่างแพร่หลาย ไม่ว่าจะเป็นเพื่อ การเรียน การค้นคว้า หรือการสื่อสาร แม้จะเป็นเครื่องมือที่มีประโยชน์ แต่หากขาดการระมัดระวังหรือขาดความ รู้เท่าทัน อาจนำไปสู่ภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อทั้งด้านร่างกาย จิตใจ และการเรียนรู้ได้โดยไม่รู้ตัว อันตรายทางไซเบอร์ที่เกิดขึ้นกับผู้เรียน มีดังนี้

1. การกลั่นแกล้งทางไซเบอร์ การกลั่นแกล้งทางไซเบอร์เป็นปัญหาที่พบบ่อยในกลุ่มผู้เรียน เป็นการ ใช้เทคโนโลยีเพื่อทำร้ายผู้อื่น เช่น การโพสต์ข้อความหรือรูปภาพที่ทำให้ผู้อื่นรู้สึกอับอายหรือถูกข่มขู่ ผลกระทบจาก การกลั่นแกล้งทางไซเบอร์สามารถรุนแรง ส่งผลให้ผู้เรียนเสียความมั่นใจในตนเอง เกิดภาวะเครียดหรือซึมเศร้า และอาจนำไปสู่การหลีกเลี่ยงการไปโรงเรียน

2. การล่อลวงออนไลน์ ผู้ไม่ประสงค์ดีหรือผู้ล่อลวงทางอินเทอร์เน็ตมักจะใช้โปรไฟล์ปลอมในการติดต่อกับผู้เรียน เพื่อสร้างความไว้วางใจและพยายามนำผู้เรียนไปสู่การพบปะทางกาย หรืออาจเป็นการล่อลวงให้แชร์ ข้อมูลส่วนตัวหรือภาพส่วนตัว ซึ่งอาจนำไปสู่ปัญหาทางกฎหมายและอันตรายต่อผู้เรียนได้

3. การขโมยข้อมูลส่วนตัว ผู้เรียนมักขาดความระมัดระวังในการคลิกลิงก์หรือการเปิดเผยข้อมูลส่วนตัว บนเว็บไซต์ที่ไม่น่าเชื่อถือ ซึ่งอาจนำไปสู่การขโมยข้อมูลส่วนตัว เช่น รหัสผ่าน หมายเลขบัตรเครดิต หรือข้อมูล ส่วนบุคคลที่สำคัญ ข้อมูลเหล่านี้สามารถถูกใช้เพื่อแอบอ้างหรือนำไปใช้ในทางที่ผิด

4. การเข้าถึงเนื้อหาที่ไม่เหมาะสม ผู้เรียนอาจพบเนื้อหาที่ไม่เหมาะสมบนอินเทอร์เน็ต เช่น เนื้อหาทาง เพศ ความรุนแรง หรือข้อมูลที่ผิดพลาต ซึ่งอาจส่งผลกระทบต่อพฤติกรรม ความคิด และทัศนคติของพวกเขา เนื้อหาประเภทนี้อาจกระทบต่อการพัฒนาทางอารมณ์และการเรียนรู้ของผู้เรียน

5. การเสพติดอินเทอร์เน็ตและเกมออนไลน์ การใช้อินเทอร์เน็ตและเกมออนไลน์มากเกินไปสามารถทำให้ ผู้เรียนเสพติด ซึ่งส่งผลต่อสุขภาพกายและจิตใจ เช่น การเสียสุขภาพจากการนั่งหน้าจอานาน ๆ การนอนหลับไม่ เพียงพอ และความเครียดจากการเรียนหรือการใช้ชีวิตประจำวัน

6. การถูกล่อลวงให้ทำกิจกรรมที่ไม่เหมาะสม (Catfishing and Deceptive Activities) ในบางกรณี ผู้เรียนอาจถูกล่อลวงให้เข้าร่วมกิจกรรมที่ไม่เหมาะสมหรือผิดกฎหมาย เช่น การส่งภาพหรือข้อมูลส่วนตัว การสร้าง โปรไฟล์ปลอมเพื่อหลอกลวงผู้อื่น ซึ่งอาจส่งผลเสียต่อชื่อเสียงและความปลอดภัยของพวกเขา

จากประเด็นข้างต้นสรุปได้ว่า ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับผู้เรียนในปัจจุบันมีความหลากหลายและส่งผลกระทบต่อทั้งด้านจิตใจ พฤติกรรม และความปลอดภัยส่วนบุคคล โดยเฉพาะอย่างยิ่งในกลุ่มเด็กและเยาวชนที่ใช้อินเทอร์เน็ตเป็นประจำ อันตรายที่พบบ่อย ได้แก่ การกลั่นแกล้งทางไซเบอร์ ซึ่งส่งผลให้ผู้เรียนรู้สึกเครียด ขาดความมั่นใจ และไม่อยากไปโรงเรียน การล่อลวงออนไลน์ที่มักใช้โปรไฟล์ปลอมในการเข้าหาเหยื่อเพื่อหวังผลประโยชน์ หรือพาไปสู่สถานการณ์อันตราย รวมถึงการขโมยข้อมูลส่วนตัวจากการคลิกลิงก์หรือเปิดเผยข้อมูลบนเว็บไซต์ที่ไม่ปลอดภัย

นอกจากนี้ ผู้เรียนยังเสี่ยงต่อการเข้าถึงเนื้อหาที่ไม่เหมาะสม เช่น ภาพลามก ความรุนแรง หรือข้อมูลเท็จ ซึ่งส่งผลกระทบต่อพัฒนาการและแนวคิดของเด็ก อีกทั้งยังมีปัญหาการเสพติดอินเทอร์เน็ตและเกมออนไลน์ ซึ่งกระทบต่อสุขภาพและการเรียนรู้ รวมถึงการถูกล่อลวงให้ทำกิจกรรมที่ไม่เหมาะสมหรือผิดกฎหมาย เช่น การส่งภาพส่วนตัวหรือสร้างโปรไฟล์ปลอม ภัยคุกคามทางไซเบอร์เป็นปัญหาที่ต้องตระหนักและเฝ้าระวัง โดยเฉพาะในกลุ่มผู้เรียนที่ยังขาดวุฒิภาวะในการแยกแยะความปลอดภัยทางโลกออนไลน์ จำเป็นต้องมีการให้ความรู้และสร้างเกราะป้องกันที่เหมาะสมจากทั้งครอบครัว โรงเรียน และสังคม

แนวทางการพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์

ความปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึง กระบวนการในการนำเทคโนโลยีมาใช้ เพื่อปกป้องเด็กประถมศึกษาจากอันตรายที่เกิดขึ้นในเครือข่าย ไม่ว่าจะเป็นจากการถูกโจรกรรมหรือข้อมูลสูญหายจาก เหตุที่ไม่สามารถควบคุมได้ เช่น การที่บุคคลสร้างโปรแกรมหรือเครื่องมือบางอย่างเพื่อเป้าหมายในการส่งผลกระทบต่อคนละคนหรือองค์กรเป็นสำคัญ โดยภัยดังกล่าวแบ่งออก 3 ประเภทหลัก (Cyber Security Threats) คือ

ประเภทที่ 1 อาชญากรรมไซเบอร์ (Cybercrime) ที่เป็นการกระทำของบุคคลหรือโปรแกรมที่ทำให้องค์กรหรือบุคคลเกิดความเสียหาย เพื่อหาผลประโยชน์ทางการเงิน ตัวอย่างเช่น การเจาะระบบเข้าสู่ข้อมูล หรือการสร้างระบบหลอกจ่ายเงิน เป็นต้น

ประเภทที่ 2 คือ การโจมตีผ่านไซเบอร์ (Cyber - attack) ที่หมายถึง การกระทำโดยโปรแกรมหรือ กลุ่มคนเพื่อปลอมแปลงหรือปรับเปลี่ยนระบบ และนำข้อมูลไปทำการอย่างใดอย่างหนึ่ง เช่น การเจาะระบบของสถานศึกษาเพื่อโจรกรรมข้อมูลนักศึกษาทำธุรกรรมทางการเงิน หรือการเจาะระบบตลาดหุ้น เพื่อปลอมแปลงราคา เป็นต้น

ประเภทที่ 3 คือ การก่อการร้ายทางไซเบอร์ (Cyberterrorism) การกระทำโดยโปรแกรมหรือกลุ่มคนเพื่อสร้างความสับสน และความกลัว ให้เกิดขึ้นในจิตใจของเด็ก เช่น การส่งต่อลัทธิความเชื่อแปลก ๆ หรือการส่งข่าวที่ไม่มีมูลความจริงเพื่อให้เด็กเกิดความตื่นกลัว (วัดสาตรี ดิถียนต์, 2566)

การพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์สำหรับผู้เรียนชั้นประถมศึกษาานั้น จะแบ่งออกเป็น 2 ส่วนคือ การส่งเสริมความรู้เกี่ยวกับการสร้างความปลอดภัยทางไซเบอร์ และการพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์ สามารถอธิบายได้ดังนี้

ส่วนที่ 1 ส่งเสริมความรู้ด้านความปลอดภัยไซเบอร์

จากคุณสมบัติพื้นฐานของสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยข้างต้น สามารถแสดงให้เห็นถึงแนวทางการส่งเสริมความปลอดภัยไซเบอร์ให้เกิดขึ้นภายในตัวผู้เรียนได้เช่นกัน โดยแนวทางที่เกี่ยวข้องกับการสร้างความมั่นใจ และความพร้อมที่เกี่ยวข้องกับความรู้ความสามารถ 2 ด้านที่ผู้เรียนในยุคดิจิทัลควรมีและควรส่งเสริมให้เกิดขึ้น เพื่อเป็นเกราะป้องกันภัยอันตรายทางไซเบอร์ที่อยู่รายล้อมตนเองได้อย่างสมบูรณ์และยั่งยืนได้ต่อไป ซึ่งประกอบไปด้วย

1. การส่งเสริมความฉลาดทางดิจิทัล (Digital Intelligence)

ความฉลาดทางดิจิทัล เป็นความสามารถของบุคคลในการใช้ประโยชน์ของเทคโนโลยีต่อการทำธุรกรรมต่าง ๆ ต่อการดำรงชีวิตได้อย่างประสบความสำเร็จ ความฉลาดทางดิจิทัลแบ่งออกเป็น 3 ระดับ ประกอบไปด้วยระดับแรก คือพลเมืองดิจิทัล (Digital citizenship) หมายถึงความสามารถในการใช้เครื่องมือดิจิทัลให้ปลอดภัยและมีประสิทธิภาพเพื่อการดำเนินชีวิต ถือว่าเป็นความฉลาดทางดิจิทัลขั้นพื้นฐานที่ทุกคนควรมีและสามารถทำได้ไม่ว่าจะเป็นในช่วงอายุใดก็ตาม ระดับต่อมา คือ ความคิดสร้างสรรค์ทางดิจิทัล (Digital creativity) การที่บุคคลสามารถนำตนเองเข้ามาเป็นส่วนหนึ่งของระบบหรือสภาพแวดล้อมดิจิทัลได้ ผ่านการสร้างสรรค์เนื้อหาหรือองค์ความรู้ใหม่ที่จะไปพัฒนาต่อยอด และเห็นผลเชิงประจักษ์ได้ในชีวิตจริงผ่านการใช้เครื่องมือดิจิทัลเป็นความสามารถที่ควรส่งเสริม และพัฒนาให้เกิดขึ้นผู้เรียน และระดับสุดท้าย การประกอบการดิจิทัล (Digital entrepreneurship) หมายถึง ความสามารถของบุคคลในการใช้เครื่องมือดิจิทัลเพื่อแก้ปัญหาในระดับสากล รวมถึงการสร้างโอกาสและความท้าทายใหม่ ๆ ให้เกิดขึ้นในสังคมผ่านการใช้เครื่องมือดิจิทัล โดยเป็นความสามารถที่ควรส่งเสริมอย่างต่อเนื่องให้เกิดขึ้นแก่ผู้เรียนในปัจจุบันและอนาคต (สรานนท์ อินทนนท์, 2563 และ DQ Institute, 2019) ได้อธิบายความสามารถ 8 ด้านที่ผู้สอนควรส่งเสริมให้เกิดขึ้นเพื่อภายในตัวผู้เรียนเพื่อส่งเสริมให้เกิดความฉลาดทางดิจิทัล ประกอบด้วย



ภาพที่ 2 ความฉลาดทางดิจิทัล

ที่มา : มูลนิธิส่งเสริมสื่อเด็กและเยาวชน (2563)

1. ทักษะการรักษาอัตลักษณ์ที่ดีของตนเองในโลกดิจิทัล (Digital Citizen's Identity) ผู้เรียนควรรู้จักวิธีสร้างและรักษาอัตลักษณ์ในโลกออนไลน์อย่างปลอดภัยและเป็นบวก เช่น การใช้ชื่อผู้ใช้งานและรูปโปรไฟล์ที่เหมาะสม รวมถึงการมีมารยาทในการสื่อสารออนไลน์ โดยควรแสดงความเคารพและเห็นใจเพื่อนร่วม

สังคมออนไลน์ ตระหนักถึงผลกระทบจากการโพสต์เนื้อหา ไม่ละเมิดลิขสิทธิ์ ไม่กลั่นแกล้งทางออนไลน์ และหลีกเลี่ยงการใช้คำพูดที่ไม่เหมาะสม

2. ทักษะการคิดวิเคราะห์และมีวิจารณญาณ (Critical Thinking) ผู้เรียนควรสามารถแยกแยะข้อมูลที่น่าเชื่อถือและข้อมูลที่น่าเป็นอันตรายได้ เช่น เข้าใจว่าเนื้อหาข่าวสารใดมีประโยชน์และควรเชื่อถือ หรือสังเกตความผิดปกติที่น่าเป็นข่าวปลอมหรือเว็บไซต์หลอกลวง การรู้เท่าทันสื่อและสารสนเทศจะช่วยให้ผู้เรียนป้องกันตัวเองจากข้อมูลที่ไม่ถูกต้อง

3. ทักษะในการรักษาความปลอดภัยในโลกไซเบอร์ (Cybersecurity Management) ผู้เรียนควรมีทักษะในการรักษาความปลอดภัยข้อมูลของตนเอง เช่น ตั้งรหัสผ่านที่ปลอดภัย ไม่เปิดเผยข้อมูลส่วนตัว และไม่คลิกลิงก์ที่น่าสงสัย ทักษะนี้จะช่วยป้องกันไม่ให้ข้อมูลส่วนตัวถูกนำไปใช้ในทางที่ไม่เหมาะสมและป้องกันการโจรกรรมข้อมูลทางออนไลน์

4. ทักษะการจัดการข้อมูลส่วนตัว (Privacy Management) การรู้จักป้องกันข้อมูลส่วนตัวเป็นเรื่องสำคัญ เช่น การไม่เปิดเผยข้อมูลส่วนตัวโดยไม่จำเป็น การระมัดระวังในการแชร์รูปภาพและข้อมูลต่าง ๆ เพื่อให้ผู้ไม่หวังดีนำข้อมูลส่วนตัวไปใช้ในทางที่ไม่ถูกต้อง ผู้เรียนควรตระหนักถึงภัยคุกคามเช่น มัลแวร์และไวรัสคอมพิวเตอร์ และหลีกเลี่ยงการดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ

5. ทักษะในการจัดการเวลาในการใช้หน้าจอ (Screen Time Management) ผู้เรียนควรรู้จักควบคุมเวลาที่ใช้กับหน้าจออุปกรณ์ดิจิทัล เพื่อไม่ให้ส่งผลกระทบต่อสุขภาพทั้งกายและใจ ควรแบ่งเวลาระหว่างการทำกิจกรรมออนไลน์และกิจกรรมนอกบ้านอย่างสมดุล และหลีกเลี่ยงการทำกิจกรรมหลายอย่างพร้อมกันเพื่อลดความเครียดและความเหนื่อยล้า

6. ทักษะการจัดการร่องรอยข้อมูลที่ทิ้งไว้ในโลกออนไลน์ (Digital Footprints) ผู้เรียนควรเข้าใจว่าการกระทำบนโลกออนไลน์ เช่น การโพสต์รูปภาพหรือข้อความ จะทิ้งร่องรอยข้อมูลไว้ แม้จะลบออกไปแล้วก็อาจถูกติดตามหรือกู้คืนได้ ดังนั้นผู้เรียนควรระมัดระวังในการโพสต์เนื้อหา เพื่อป้องกันไม่ให้สิ่งที่โพสต์ส่งผลเสียต่อภาพลักษณ์ของตนเองในอนาคต

7. ทักษะการรับมือกับการกลั่นแกล้งบนโลกไซเบอร์ (Cyberbullying Management) การกลั่นแกล้งบนโลกไซเบอร์เป็นสิ่งที่สามารถเกิดขึ้นได้ง่ายและรุนแรงต่อผู้เรียน การรับมือที่ถูกต้องคือต้องไม่ตอบโต้ผู้กลั่นแกล้ง ออกจากบัญชีสื่อสังคมออนไลน์หรือปิดการสื่อสารชั่วคราว หากยังถูกกลั่นแกล้ง ควรแจ้งให้ผู้ปกครองหรือครูทราบ และใช้ฟังก์ชันบล็อกผู้ใช้งานในสื่อสังคมออนไลน์เพื่อป้องกันการถูกรบกวนเพิ่มเติม

8. ทักษะการใช้เทคโนโลยีอย่างมีจริยธรรม (Digital Empathy) การใช้อินเทอร์เน็ตอย่างมีจริยธรรมหมายถึง การมีความเห็นอกเห็นใจและเข้าใจผู้อื่นบนโลกออนไลน์ ไม่ดวนดัดสินเพื่อนจากข้อมูลที่เห็นทางอินเทอร์เน็ตเพียงอย่างเดียว และสามารถแสดงออกถึงความสนับสนุนหรือช่วยเหลือผู้อื่นหากมีความจำเป็น ทักษะนี้จะช่วยให้ผู้เรียนมีความสัมพันธ์ที่ดีต่อเพื่อนทั้งในโลกออนไลน์และในชีวิตจริง

จากประเด็นข้างต้นสรุปได้ว่า การส่งเสริมความฉลาดทางดิจิทัล คือ ความสามารถในการใช้เทคโนโลยีดิจิทัลอย่างปลอดภัย มีประสิทธิภาพ และเกิดประโยชน์ในการดำเนินชีวิตประจำวัน โดยแบ่งออกเป็น 3 ระดับ คือ 1) พลเมืองดิจิทัล ความสามารถพื้นฐานในการใช้งานเครื่องมือดิจิทัลอย่างปลอดภัยและมีความรับผิดชอบ 2) ความคิดสร้างสรรค์ทางดิจิทัล การมีส่วนร่วมในการสร้างสรรค์เนื้อหา และใช้เทคโนโลยีในการพัฒนาองค์ความรู้ใหม่ 3) การประกอบการดิจิทัล (Digital Entrepreneurship) การใช้เครื่องมือดิจิทัลเพื่อสร้างนวัตกรรม แก้ปัญหา และสร้างโอกาสในระดับสากล นอกจากนี้ ยังมีทักษะสำคัญ 8 ด้านที่ควรส่งเสริมในผู้เรียนเพื่อพัฒนาความฉลาดทางดิจิทัล ได้แก่ 1) การรักษาอัตลักษณ์ในโลกดิจิทัล ใช้ชื่อผู้ใช้ รูปโปรไฟล์ และพฤติกรรมออนไลน์อย่างเหมาะสม 2) การคิดวิเคราะห์และมีวิจารณญาณ แยกแยะข้อมูลจริง ข่าวปลอม และสื่อที่เป็นอันตราย 3) การรักษาความปลอดภัยทางไซเบอร์ เช่น การตั้งรหัสผ่านที่ปลอดภัยและหลีกเลี่ยงลิงก์น่าสงสัย 4) การจัดการข้อมูลส่วนตัว ระวัง

การเปิดเผยข้อมูลหรือรูปภาพที่อาจถูกนำไปใช้ในทางที่ผิด 5) การจัดการเวลาใช้หน้าจอ ควบคุมเวลาใช้งาน อุปกรณ์ดิจิทัลอย่างสมดุล เพื่อสุขภาพที่ดี 6) การจัดการร่องรอยข้อมูล (Digital Footprint) ตระหนักว่าทุกโพสต์อาจมีผลในอนาคต 7) การรับมือกับการกลั่นแกล้งออนไลน์ ไม่ตอบโต้ ใช้เครื่องมือบล็อก และแจ้งผู้ใหญ่เมื่อจำเป็น 8) การใช้อินเทอร์เน็ตอย่างมีจริยธรรม แสดงความเข้าใจ เห็นอกเห็นใจ และช่วยเหลือผู้อื่นในโลกออนไลน์ การส่งเสริมความฉลาดทางดิจิทัลให้กับผู้เรียนเป็นสิ่งสำคัญอย่างยิ่งในยุคเทคโนโลยี เพื่อให้พวกเขาใช้สื่อดิจิทัลอย่างสร้างสรรค์ ปลอดภัย มีจริยธรรม และสามารถพัฒนาตนเองให้พร้อมต่อโลกอนาคตได้อย่างยั่งยืน

2. การส่งเสริมความฉลาดทางอารมณ์ (Emotional Intelligence)

ความฉลาดทางอารมณ์ของเด็กสามารถนำมาประยุกต์ใช้กับการพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์ เพื่อให้พวกเขามีความพร้อมทั้งทางอารมณ์และการใช้เทคโนโลยีอย่างปลอดภัย ซึ่งจะช่วยให้เด็กผู้เรียนชั้นประถมศึกษาเรียนรู้ที่จะใช้อินเทอร์เน็ตและเทคโนโลยีต่าง ๆ อย่างมีความรับผิดชอบและลดความเสี่ยงจากภัยคุกคามในโลกไซเบอร์ได้ (กรมสุขภาพจิต, 2550) ให้ความหมายของ ความฉลาดทางอารมณ์ว่า ความสามารถทางอารมณ์ ในการดำเนินชีวิตร่วมกับผู้อื่นอย่างสร้างสรรค์และมีความสุข ประกอบด้วยปัจจัยคุณภาพที่สำคัญ 3 ปัจจัย คือ 1) ความดี ความสามารถในการควบคุมอารมณ์และความต้องการของตนเอง รู้จักเห็นใจผู้อื่น และมีความรับผิดชอบต่อส่วนรวม 2) ความเก่ง ความสามารถในการรู้จักตนเอง สามารถตัดสินใจแก้ปัญหา รวมทั้งการแสดงออกได้อย่างมีประสิทธิภาพตลอดจนมีความสัมพันธ์ที่ดีกับผู้อื่น 3) ความสุข ความสามารถในการดำรงชีวิตอย่างเป็นสุข ภูมิใจในตนเอง และพอใจในชีวิต (ฐิติพร ศุภสิทธิ์ธำรง, 2566) กล่าวว่า ความฉลาดทางอารมณ์สามารถจำแนกออกได้เป็น 5 ประการ ได้แก่

1.การตระหนักรู้และเข้าใจอารมณ์ของตนเอง (Self-Awareness) ผู้เรียนควรรู้จักอารมณ์ของตนเอง เมื่อเผชิญกับสถานการณ์ทางไซเบอร์ เช่น รู้สึกตื่นเต้นเมื่อได้รับข้อความใหม่ หรือตกใจเมื่อเจอเนื้อหาที่ไม่เหมาะสม การรู้จักอารมณ์ของตนเองช่วยให้เด็กสามารถหยุดคิดก่อนตอบสนองต่อข้อความหรือลิงก์ที่ไม่แน่ใจ เพื่อไม่ให้ตกเป็นเหยื่อของการหลอกลวง เช่น การคลิกลิงก์ฟิชซิงที่ส่งมาหลอกให้กรอกข้อมูลส่วนตัว

2. การจัดการอารมณ์ของตนเอง (Self-Management) ผู้เรียนควรเรียนรู้วิธีควบคุมอารมณ์เมื่อใช้งานเทคโนโลยี เช่น คิดให้ถี่ถ้วนแชร์ข้อความหรือข้อมูล โดยเฉพาะเมื่อรู้สึกโกรธหรือหงุดหงิด การจัดการอารมณ์ช่วยลดความเสี่ยงจากการส่งต่อข่าวลือหรือข้อมูลที่อาจสร้างความเสียหายได้ และยังสามารถตอบโต้กับความท้าทายทางออนไลน์ได้อย่างมีเหตุผล

3. การเข้าใจและเห็นอกเห็นใจผู้อื่น (Social Awareness) ผู้เรียนควรเรียนรู้ที่จะเข้าใจและเห็นใจผู้อื่นในโลกไซเบอร์ เช่น การไม่แสดงพฤติกรรมรังแก (Cyberbullying) และการให้กำลังใจเพื่อนที่อาจตกอยู่ในสถานการณ์ไม่ดีบนออนไลน์ รวมถึงการระวังและเตือนเพื่อน ๆ เมื่อพบเห็นสิ่งที่เป็นอันตราย การเห็นใจผู้อื่นช่วยสร้างสภาพแวดล้อมออนไลน์ที่ปลอดภัยและเป็นมิตร

4. การสร้างและรักษาความสัมพันธ์ที่ดี (Relationship Management) ผู้เรียนควรเรียนรู้วิธีสร้างความสัมพันธ์ทางออนไลน์ที่ดี เช่น การพูดคุยสุภาพกับเพื่อน การเคารพความคิดเห็นของผู้อื่น และหลีกเลี่ยงการโพสต์หรือส่งข้อความที่อาจสร้างความขัดแย้ง การรักษาความสัมพันธ์ที่ดีจะช่วยให้การทำงานหรือการเรียนรู้ร่วมกันทางออนไลน์มีประสิทธิภาพและเกิดบรรยากาศที่ดี

5. การสร้างแรงจูงใจให้ตนเอง (Self-Motivation) ผู้เรียนควรสร้างแรงจูงใจในการเรียนรู้เรื่องความปลอดภัยทางไซเบอร์ เช่น ตั้งเป้าหมายในการเรียนรู้เกี่ยวกับการป้องกันภัยคุกคามทางออนไลน์ หรือการฝึกฝน

ทักษะความปลอดภัย เช่น การจำรหัสผ่านให้ดี การไม่เปิดเผยข้อมูลส่วนตัว หรือการระวังการใช้ข้อมูลออนไลน์อย่างปลอดภัย การมีแรงจูงใจและความตั้งใจจะช่วยให้เด็กพัฒนาความปลอดภัยทางไซเบอร์อย่างต่อเนื่อง

จากประเด็นข้างต้นสรุปได้ว่า การส่งเสริมความฉลาดทางอารมณ์เป็นทักษะสำคัญที่ช่วยให้ผู้เรียนใช้เทคโนโลยีอย่างปลอดภัยและมีความรับผิดชอบ โดยประกอบด้วย 5 ด้านหลัก ได้แก่ การรู้จักและเข้าใจอารมณ์ของตนเอง การควบคุมอารมณ์เมื่อเผชิญสถานการณ์ต่าง ๆ บนโลกออนไลน์ การเข้าใจและเห็นใจผู้อื่น การสร้างความสัมพันธ์ที่ดีผ่านการสื่อสารอย่างสุภาพ และการมีแรงจูงใจในการเรียนรู้เกี่ยวกับความปลอดภัยไซเบอร์ การพัฒนาทักษะเหล่านี้จะช่วยให้ผู้เรียนสามารถรับมือกับภัยทางไซเบอร์ได้อย่างมีสติ ลดความเสี่ยงจากพฤติกรรมไม่เหมาะสม และสร้างสภาพแวดล้อมออนไลน์ที่ปลอดภัย

ส่วนที่ 2 การพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์

การพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์นั้น หลักการสำคัญ คือ ผู้เรียนต้องเข้าใจว่าพฤติกรรมใดเสี่ยง และรู้วิธีหลีกเลี่ยงและจำกัดความเสี่ยงนั้นความเสี่ยงนั้นได้แก่ ความเสี่ยงจากพฤติกรรมการใช้งาน (Behavioral Risks) ความเสี่ยงจากเนื้อหา (Content Risks) ความเสี่ยงจากการติดต่อกับคน (Contact Risks) โดยการใช้ Interland คือ เกมออนไลน์ที่เต็มไปด้วยการผจญภัยที่จะทำให้การเรียนรู้เกี่ยวกับความปลอดภัยและการเป็นพลเมืองยุคดิจิทัลเป็นเรื่องที่สนุกสนานและเต็มไปด้วยปฏิสัมพันธ์เหมือนกับการท่องโลกอินเทอร์เน็ต สำหรับเกมนี้ ผู้เรียน จะได้ช่วยเหลือเพื่อนนักท่องโลกอินเทอร์เน็ตคนอื่นๆ ต่อสู้กับแฮกเกอร์ นักฟิชซิง คนที่แชร์มากเกินไป และวายร้ายที่ขบถกลับแก๊งผู้อื่นด้วยการฝึกฝนทักษะที่จำเป็นต่อการเป็นพลเมืองดิจิทัลที่ดี โดยเน้นไปที่ 4 ทักษะหลัก ซึ่งแต่ละทักษะจะมีรูปแบบเกมที่เฉพาะเจาะจง ทำให้การเรียนรู้เรื่องความปลอดภัยทางไซเบอร์เป็นเรื่องสนุกและเข้าใจง่าย ดังนี้:

1. Be Internet Smart (คิดก่อนแชร์)

เกมในส่วนนี้สอนให้ผู้เรียนเข้าใจเรื่องความจริงและความเท็จในโลกออนไลน์ ฝึกให้พวกเขาตรวจสอบแหล่งที่มาของข้อมูลและคิดให้รอบคอบก่อนแชร์ข้อมูล การใช้เกมทำให้ผู้เรียนเห็นผลกระทบจากการเผยแพร่ข้อมูลที่อาจไม่เป็นความจริง และเรียนรู้ที่จะระมัดระวังในเรื่องของข่าวปลอม (Fake News) และการหลอกลวงบนอินเทอร์เน็ต ข่าวต่างๆ (ทั้งดีและไม่ดี) แพร่กระจายในโลกอินเทอร์เน็ตได้อย่างรวดเร็ว และหากไม่คิดให้รอบคอบ ผู้เรียน อาจตกอยู่ในสถานการณ์ที่ลำบากและมีผลกระทบในระยะยาว ดูวิธีแชร์ข้อมูลกับคนที่รู้จักและไม่รู้จักได้สื่อสารอย่างมีความรับผิดชอบ ส่งเสริมการคิดก่อนแชร์โดยใช้หลักคิดง่าย ๆ ว่าการสื่อสารออนไลน์ก็เหมือนกับการสื่อสารแบบตัวต่อตัว ถ้าไม่ใช่เรื่องที่น่าพูด ก็แปลว่าไม่ใช่เรื่องที่น่าโพสต์ สร้างคู่มือเกี่ยวกับประเภทการสื่อสารที่เหมาะสม (และไม่เหมาะสม) เก็บรายข้อมูลเกี่ยวกับครอบครัวและเพื่อน ๆ ไว้เป็นความลับ

2. Be Internet Alert (ไม่ตกหลุมพรางกลลวง)

ส่วนนี้มุ่งเน้นให้ผู้เรียนเรียนรู้เกี่ยวกับการหลอกลวง เช่น การฟิชซิง (Phishing) และการขโมยข้อมูล เกมจะช่วยให้ผู้เรียนเรียนรู้วิธีป้องกันตัวจากการถูกขโมยข้อมูลส่วนตัว และรู้จักวิธีตรวจสอบและหลีกเลี่ยงลิงก์หรือลิงก์ที่อาจเป็นอันตราย เป็นการเสริมสร้างทักษะในการระมัดระวังและป้องกันตนเองจากภัยคุกคามทางไซเบอร์ รู้เท่าทันสัญญาณของกลโกง ถ้าเห็นคำว่า "ชนะรางวัล" หรือได้รับของ "ฟรี" แล้วรู้สึกได้ว่าดีเกินกว่าที่จะเป็นไปได้ ส่วนใหญ่ก็เป็นกับดักที่ขุดมาล่อเรา การแลกเปลี่ยนที่ยุติธรรมไม่ควรมีเรื่องข้อมูลส่วนตัวมาเกี่ยวข้อง คิดอย่างรอบคอบทุกครั้งก่อนที่จะทำอะไรในโลกออนไลน์ และเรียนรู้ที่จะเชื่อมั่นในสัญชาตญาณของตนเอง ระแวดระวังการฟิชซิง ซึ่งก็คือการพยายามขโมยข้อมูลต่างๆ เช่น รายละเอียดการเข้าสู่ระบบหรือบัญชี โดยปลอมตัวเป็นคนที่ดูน่าเชื่อถือในอีเมล ข้อความ หรือการสื่อสารออนไลน์อื่นๆ

3. Be Internet Strong (เก็บข้อมูลไว้เป็นความลับ)

ในส่วนนี้ Interland จะสอนให้ผู้เรียนเข้าใจความสำคัญของการใช้รหัสผ่านที่แข็งแกร่งและยากต่อการคาดเดา เกมจะให้คำแนะนำเกี่ยวกับการสร้างรหัสผ่านที่ดี เช่น การใช้ตัวอักษรผสมกันทั้งตัวใหญ่ ตัวเล็ก ตัวเลข และสัญลักษณ์ การทำให้ผู้เรียน ตระหนักถึงการตั้งรหัสผ่านที่ปลอดภัยสามารถช่วยป้องกันข้อมูลสำคัญของพวกเขามาจากการถูกเจาะเข้าระบบ ความเป็นส่วนตัวและความปลอดภัยส่วนบุคคลในโลกออนไลน์และออฟไลน์นั้นก็สำคัญไม่แพ้กัน การปกป้องข้อมูลที่สำคัญช่วยให้ผู้เรียน หลีกเลี่ยงการสร้างความเสี่ยงต่ออุปกรณ์ ชื่อเสียง และความสัมพันธ์ได้ สร้างรหัสผ่านที่จำได้ง่ายแต่หลีกเลี่ยงการใช้ข้อมูลส่วนตัว อย่าใช้รหัสผ่านเดียวกันในหลายเว็บไซต์ สร้างรหัสผ่านให้แตกต่างกันสำหรับใช้กับบัญชีแต่ละบัญชี

4. Be Internet Kind (ใช้อินเทอร์เน็ตอย่างมีน้ำใจ)

ทักษะนี้เน้นการสร้างสภาพแวดล้อมออนไลน์ที่เป็นมิตรและปลอดภัย สอนให้ผู้เรียนเรียนรู้เรื่องการกลั่นแกล้งทางออนไลน์ (Cyberbullying) และรู้วิธีปฏิบัติตัวเมื่อพบการกลั่นแกล้งออนไลน์ เกมนี้ช่วยส่งเสริมให้ผู้เรียน ปฏิบัติตนบนโลกออนไลน์อย่างสุภาพ มีน้ำใจ และสนับสนุนให้เกิดสังคมออนไลน์ที่เป็นมิตร อินเทอร์เน็ตเป็นกระบอกเสียงอันทรงพลังในการเผยแพร่เรื่องที่ดีและไม่ดี ช่วยให้ผู้เรียน เลือกทางที่ถูกต้องโดยใช้แนวคิด “จงปฏิบัติต่อผู้อื่นเหมือนที่อยากให้ผู้อื่นปฏิบัติต่อตัวเรา” กับการทำสิ่งต่างๆ ในโลกออนไลน์ ซึ่งจะช่วยให้ได้ผลลัพธ์ที่ดีสำหรับผู้อื่นและกำจัดพฤติกรรมการกลั่นแกล้งให้หมดไป ใช้พลังของอินเทอร์เน็ตในการส่งพลังทางบวกให้คนรอบข้าง หยุดการแพร่กระจายข้อความที่เป็นอันตรายหรือเป็นเท็จโดยการไม่ส่งต่อให้ผู้อื่น เคารพในความแตกต่างของผู้อื่น บล็อกพฤติกรรมที่น่ารังเกียจหรือไม่เหมาะสมทางออนไลน์ ยินยอมเพื่อสนับสนุนผู้ที่ถูกกลั่นแกล้ง สนับสนุนให้ผู้เรียน กล่าวตักเตือนและรายงานการกลั่นแกล้งในโลกออนไลน์

บทสรุป

การพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์สำหรับผู้เรียนประถมศึกษา มุ่งเน้นการเตรียมความพร้อมให้ผู้เรียน รู้จักและระมัดระวังภัยอันตรายที่อาจพบเจอในโลกออนไลน์ การพัฒนาทักษะเหล่านี้จะช่วยให้ผู้เรียน ป้องกันตนเองจากการถูกกลั่นแกล้ง ล่อลวง และการสูญเสียข้อมูลส่วนตัว รวมถึงการหลีกเลี่ยงเนื้อหาที่ไม่เหมาะสม แนวทางการพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์แบ่งออกเป็นสองส่วน ได้แก่ ส่วนที่หนึ่ง การส่งเสริมความรู้ด้านความปลอดภัยในโลกไซเบอร์ และการพัฒนาความฉลาดทางดิจิทัลและความฉลาดทางอารมณ์ ในส่วนของความฉลาดทางดิจิทัลนั้น ประกอบด้วยทักษะที่จำเป็น อาทิ การตระหนักและดูแลรักษาอัตลักษณ์ในโลกออนไลน์ การคิดวิเคราะห์ข้อมูลเพื่อแยกแยะความถูกต้อง การจัดการข้อมูลส่วนบุคคลอย่างปลอดภัย และการจัดสรรเวลาในการใช้สื่อดิจิทัลอย่างสมดุล ส่วนการพัฒนาความฉลาดทางอารมณ์มุ่งเน้นให้เยาวชนรู้จักควบคุมและจัดการอารมณ์ของตนเอง รวมถึงการสร้างแรงจูงใจในการทำกิจกรรมเชิงบวกในโลกดิจิทัล ส่วนที่สอง การพัฒนาทักษะด้านความปลอดภัยทางไซเบอร์ โดยใช้กิจกรรมการเรียนรู้เกม Interland ได้รับการออกแบบให้ผู้เรียนสามารถฝึกฝนทักษะด้านความปลอดภัยทางไซเบอร์ผ่านการเล่นเกม ตัวอย่างเช่น การฝึกทักษะคิดก่อนแชร์ข้อมูล การตรวจสอบแหล่งที่มาของข้อมูล การตั้งรหัสผ่านที่ปลอดภัย และการป้องกันตนเองจากการกลั่นแกล้งทางออนไลน์ กิจกรรมเหล่านี้ช่วยให้การเรียนรู้เรื่องความปลอดภัยทางไซเบอร์เป็นไปอย่างสนุกสนาน เข้าถึงง่าย และส่งเสริมการมีส่วนร่วมอย่างมีประสิทธิภาพ

บรรณานุกรม

- กนกวรรณ อินทปรีชา. (2564). บทบาทของการศึกษาในการเสริมสร้างความปลอดภัยทางไซเบอร์ในกลุ่มเยาวชน. วารสารวิชาการเทคโนโลยีสารสนเทศ, 8(1), 23-36.
- ญาสินี เกิดผลเสรีรัฐ. (2565). การพัฒนาทักษะการเรียนรู้สู่พลเมืองดิจิทัล. วารสารวิชาการ กสทช., 354 – 379. https://so04.tci-thaijo.org/index.php/NBTC_Journal/article/view/260058/177102
- ฐิติพร ศุภสิทธิ์ธารัง (2566). EQ (Emotional quotient) ความฉลาดทางอารมณ์. สืบค้น 30 ตุลาคม 67 : <https://www.medparkhospital.com/lifestyles/eq-emotional-quotient>
- วัดสาตรี ดิถียนต์ (2567). แนวทางการส่งเสริมความสามารถในการสร้างความปลอดภัยทางไซเบอร์สำหรับผู้เรียน. วารสารวิชาการมหาวิทยาลัยการกีฬาแห่งชาติ, 16(1) 291 – 302. <https://he02.tci-thaijo.org/index.php/TNSUJournal/article/view/262006/182325>
- ศุภณัฐ เพิ่มพูนวิวัฒน์ และคณะ (2564). ความเป็นพลเมือง: บทสำรวจสถานะความเป็นพลเมืองกับการรู้ดิจิทัล. สำนักส่งเสริมการเมืองภาคพลเมือง สถาบันพระปกเกล้า. [https://www.kpi.ac.th/knowledge/sranant%20intnnt%20\(2563\).%20ความฉลาดทางดิจิทัล.กรุงเทพฯ: วอล์คอนคลาเวต์.](https://www.kpi.ac.th/knowledge/sranant%20intnnt%20(2563).%20ความฉลาดทางดิจิทัล.กรุงเทพฯ: วอล์คอนคลาเวต์.)
- อนุกุล ปิดแก้ว. (2565). การสำรวจสถานการณ์เด็กกับภัยออนไลน์. กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์. สืบค้น 30 ตุลาคม 67 : https://www.m-society.go.th/ewtadmin/ewt/MSO_WEB_NEW/news_view.php?nid=34491.
- DQ Institute. (2019). DQ global standards report 2019: Common framework for digital literacy, skills, and readiness. <https://www.dqinstitute.org/wp-content/uploads/2019/11/DQGlobalStandardsReport2019.pdf>
- Park, Y. H. (2023). *Child Online Safety Index reveals a persistent cyber pandemic*. DQ Institute. Retrieved from <https://www.dqinstitute.org/news-post/child-online-safety-index-reveals-a-persistent-cyber-pandemic/>