แนวทางในการส่งเสริมความสามารถในการสร้างความปลอดภัยทางไซเบอร์สำหรับผู้เรียน

วัตสาตรี ดิถียนต์
ภาควิชาเทคโนโลยีการศึกษา คณะศึกษาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

บทคัดย่อ

การสร้างความปลอดภัยทางไซเบอร์ (Cyber Security) กำลังเป็นประเด็นที่สถาบันการศึกษาหรือหน่วยงานที่เกี่ยวข้องควรต้องให้ความสำคัญ เนื่องจากผู้เรียนในปัจจุบันมีความจำเป็นต้องใช้เทคโนโลยีในการเรียนตลอดเวลา ทั้งนี้ ภัยทางไซเบอร์นั้นมีหลากหลาย ไม่ว่าจะเป็นการกลั่นแกล้งทางไซเบอร์หรือการปลอมแปลงทางดิจิทัล ที่ต่างส่งผลกระทบต่อจิตใจของผู้เรียนอันนำไปสู่การออกนอกระบบการศึกษาหรือการฆ่าตัวตายได้ในที่สุด โดยแนวทางในการส่งเสริมความปลอดภัยทางไซเบอร์นั้น นอกเหนือจากการที่สถานศึกษาได้นำเครื่องมือต่างๆ มาใช้ในการคัดกรองหรือตรวจสอบแล้ว การส่งเสริมความรู้ความสามารถที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์ให้เกิดขึ้นภายในตัวผู้เรียนนั้นก็เป็นแนวทางในการป้องกันภัยเหล่านั้นได้อย่างยั่งยืนเช่นกัน ซึ่งบทความนี้จะเป็นการรวมรวมข้อมูลที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์เพื่อนำไปสู่การวิเคราะห์เพื่อหาแนวทางที่เหมาะสมต่อการส่งเสริมความปลอดภัยทางไซเบอร์ภายในตัวผู้เรียนได้ต่อไป ซึ่งจากการรวบรวมข้อมูลพบว่า แนวทางที่สำคัญนั้นประกอบไปด้วย การสร้างสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยแก่ผู้เรียน และการสร้างความรู้ความสามารถด้านความปลอดภัยทางไซเบอร์ให้เกิดขึ้นภายในตัวผู้เรียนที่ประกอบไปด้วย 1) การส่งเสริมทักษะการรู้เท่าทันสื่อที่จะช่วยให้ผู้เรียนสามารถตรวจสอบและวิเคราะห์ข้อมูลทางไซเบอร์ว่ามีความน่าเชื่อถือเพียงใด ต่อมาคือ 2) ส่งเสริมความฉลาดทางดิจิทัลที่จะช่วยให้ผู้เรียนได้เข้าใจและการใช้พลังประโยชน์ของเทคโนโลยีหรือแหล่งข้อมูลทางไซเบอร์ต่อการเรียนได้อย่างประสบความสำเร็จ และ 3) ความฉลาดทางอารมณ์ ที่ช่วยให้ผู้เรียนสามารถจัดการความรู้สึกนึกคิดและการแสดงออกของตนเองได้อย่างเหมาะสมและเกิดความปลอดภัยต่อตนเองในสภาพแวดล้อมทางไซเบอร์ได้ต่อไป

คำสำคัญ: ความปลอดภัยทางไซเบอร์; การรู้เท่าทันสื่อ; ความฉลาดทางดิจิทัล; ความฉลาดทางอารมณ์; การเรียนการสอนทางไซเบอร์

Corresponding Author: วัตสาตรี ดิถียนต์ ภาควิชาเทคโนโลยีการศึกษา คณะศึกษาศาสตร์ มหาวิทยาลัยเกษตรศาสตร์
Email: feduwtd@ku.ac.th

APPROACHES FOR ENHANCING CYBER SECURITY AMONG LEARNERS

Watsatree Diteeyon
Department of Educational Technology, Faculty of Education, Kasetsart University

Abstract

Cyber security is one of the critical issues among learners nowadays because technology has becomes the main tool of their learning. At present, there are several types of cyber harassment such as cyberbullying or digital impersonation which those become cause of learning loss or suicide issues among learners. Besides applying protection tools, increasing knowledge and abilities among learners regarding cyber security are also effective approach for improving cyber security. According to the reviews, building a secure digital learning environment is the first possible approach to increase cyber security. The next is to increase knowledge and skills in 3 different areas which are 1) media and information literacy which encourages learners to be able to analyze the validity and reliability of cyber information, 2) digital intelligence which allows learners to recognize and use technology for supporting their learning successfully, and 3) emotion intelligence that enhances learners to be able to manage and share their appropriate attitude and performance within the cyber environment.

Keywords: Cyber Security; Media and Information Literacy; Digital Intelligence; Emotional Intelligence, Cyber Education

Corresponding Author: Miss. Watsatree Diteeyont, Department of Educational Technology, Faculty of Education, Kasetsart University Email: feduwtd@ku.ac.th

บทนำ

ผลกระทบจากการแพร่ระบาดได้ทำให้รูปแบบการเรียนการสอนในประเทศไทยเข้าสู่ระบบการศึกษาแบบดิจิทัลอย่างชัดเจนมากขึ้น ดังนั้น จึงมีความจำเป็นที่ระบบการศึกษาจะต้องมีการเตรียมความพร้อมด้านเทคโนโลยี โดยเฉพาะอย่างยิ่ง การสร้างความปลอดภัยทางไซเบอร์ (Cyber Security) ที่กำลังเป็นความรู้ความสามารถที่ควรส่งเสริม (Hard skill) ให้เกิดขึ้นเป็นอย่างมาก (Rahman, Sairi, Zizi, & Khalid, 2020) โดยเฉพาะต่อผู้เรียนในระบบการศึกษาแบบดิจิทัลที่ต่างจำเป็นต้องใช้เทคโนโลยีเพื่อการเรียนแทบตลอดเวลา ดังนั้น เป้าหมายของบทความนี้ คือ การอธิบายข้อมูลเบื้องต้นเกี่ยวกับภัยอันตรายทางไซเบอร์และแนวทางในการสร้างปลอดภัยทางไซเบอร์ ซึ่งจะเป็นพื้นฐานสำคัญแก่ผู้สอนและผู้บริหารสถาบันการศึกษาในการนำไปประยุกต์ใช้เพื่อสร้างหลักสูตรหรือบทเรียน หรือแม้กระทั่งการวางแผนในการส่งเสริมความปลอดภัยทางไซเบอร์ให้แก่ผู้เรียนได้ต่อไป

ความปลอดภัยทางไซเบอร์ (Cybersecurity) หมายถึง วิธีการ กระบวนการในการนำเทคโนโลยีมาใช้เพื่อปกป้องผู้ใช้งานจากอันตรายที่เกิดขึ้นในเครือข่าย ไม่ว่าจะเป็นจากการถูกโจรกรรมหรือข้อมูลสูญหายจากเหตุที่ไม่สามารถควบคุมได้ เช่น ภัยสงครามหรือภัยพิบัติจากธรรมชาติ และการกระทำของบุคคลในการสร้างโปรแกรมหรือเครื่องมือบางอย่างเพื่อเป้าหมายในการส่งผลกระทบด้านลบแก่ผู้อื่นหรือองค์กรเป็นสำคัญ โดยภัยดังกล่าวแบ่งออก 3 ประเภทหลัก (Cyber Security Threats) คือ ประเภทที่ 1 อาชญากรรมไซเบอร์ (Cybercrime) ที่เป็นการกระทำของบุคคลหรือโปรแกรมที่ก่อความเสียหายแก่องค์กรหรือบุคคลเพื่อหาผลประโยชน์ทางการเงิน ตัวอย่างเช่น การเจาะระบบเพื่อขายข้อมูล หรือ การสร้างระบบหลอกจ่ายเงิน เป็นต้น ประเภทที่ 2 คือ การโจมตีผ่านไซเบอร์ (Cyber - attack) ที่หมายถึง การกระทำโดยโปรแกรมหรือกลุ่มคนเพื่อปลอมแปลงหรือปรับเปลี่ยน รวมไปถึงการยึดครองระบบเพื่อนำข้อมูลไปทำการอย่างใดอย่างหนึ่ง เช่น การเจาะระบบของสถาบันการศึกษาเพื่อโจรกรรรมข้อมูลนักศึกษามาทำธุรกรรมทางการเงิน หรือการเจาะระบบตลาดหุ้นเพื่อปลอมแปลงราคาหุ้น เป็นต้น และประเภทสุดท้าย คือ การก่อการร้ายทางไซเบอร์ (Cyberterrorism) การกระทำโดยโปรแกรมหรือกลุ่มคนเพื่อสร้างความสับสน ความน่ารำคาญและความกลัวให้เกิดขึ้นในจิตใจของผู้ใช้งาน เช่น การส่งต่อลัทธิความเชื่อแปลก ๆ หรือการส่งข่าวที่ไม่มีมูลความจริงเพื่อให้สังคมเกิดความตื่นกลัว (Watsatree Diteeyont, 2023)

ภัยอันตรายทางไซเบอร์ที่เกิดขึ้นในผู้เรียน

ภัยอันตรายทางไซเบอร์ที่เกิดขึ้นในกลุ่มผู้เรียนกำลังเป็นประเด็นสำคัญที่สถาบันการศึกษาควรให้ความสำคัญในการป้องกันมิให้เกิดขึ้น ซึ่งในปัจจุบันภัยอันตรายทางไซเบอร์ที่เกิดขึ้นในกลุ่มผู้เรียนจะแบ่งออกเป็น 3 ประเภท ดังนี้

1. การกลั่นแกล้งทางไซเบอร์ (Cyberbullying) เป็นภัยอันตรายทางไซเบอร์ที่มุ่งการสร้างความอับอาย ใส่ร้าย ขู่กรรโชกหรือลบหลู่ดูถูกผู้อื่นผ่านการช่องทางสื่อสารทางสังคม (Chadwick, 2014) ซึ่งมักจะเกิดขึ้นใน 3 ช่องทางการสื่อสาร คือ ระบบข้อความทางโทรศัพท์หรืออีเมล ช่องทางสื่อสารสังคม และการกระดานสังคมออนไลน์ต่าง ๆ ซึ่งทางการกลั่นแกล้งทางไซเบอร์นี้กำลังเป็นประเด็นที่ท้าทายต่อการบริหารจัดการของระบบการศึกษาในปัจจุบันเป็นอย่างมาก (Chadwick, 2014) เพราะเป็นปัญหาที่มักจะเกิดขึ้นกับผู้เรียนตั้งแต่ประถมจนถึงมหาวิทยาลัยที่เป็นวัยที่ไวต่อความรู้สึกและให้ความสำคัญต่อความคิดเห็นจากสังคมรอบตัวที่มีต่อตนเอง ซึ่งการกลั่นแกล้งทางไซเบอร์นี้จะส่งผลกระทบต่อจิตใจของผู้ที่ถูกกระทำเป็นอย่างมาก โดยก่อให้เกิดความรู้สึกเดียวดาย ความเครียดและความกังวล ซึ่งจะส่งผลต่อเนื่องไปสู่ภาวะซึมเศร้า จนนำไปสู่การตัดสินใจในการลาออกจากระบบการศึกษา การทำร้ายตนเอง/การฆ่าตัวตาย หรือแม้แต่การทำร้ายผู้อื่นหรือสังคมในวงกว้างในที่สุด (Nixon, 2014) โดยผลการวิจัยของ ยูเดส เรย์ และเอ็กทรีเมร่า (Yudes, Rey, & Extremera, 2022) ได้ชี้ชัดว่า การกลั่นแกล้งทางไซเบอร์ได้เพิ่มมากขึ้นในทั่วโลกในระหว่างปี ค.ศ. 2015 - 2019

จากร้อยละ 6 ไปสู่ร้อยละ 46.3 นอกจากนั้น ผลการวิจัยยังชี้ชัดว่าเด็กผู้ชายจะเข้าสู่การกลั่นแกล้งทางไซเบอร์มากกว่าเด็กผู้หญิงอย่างมีนัยสำคัญอีกด้วย

สำหรับประเทศไทย ข้อมูลจากผลสำรวจดัชนีชี้วัดความปลอดภัยบนสื่อออนไลน์เด็ก (Child Online Safety Index: COSI) โดยบริษัท เอไอเอสร่วมกับสถาบัน DQ ระดับโลกทำการสำรวจจาก 450 โรงเรียนทั่วประเทศ ในปี พ.ศ. 2562 ได้แสดงให้เห็นว่า ประเทศไทยมีจำนวนการกลั่นแกล้งทางไซเบอร์อยู่ในอันดับต้นของทวีปเอเชีย และในปี พ.ศ. 2563 ประเทศไทยอยู่อันดับ 5 ของโลกที่มีการกลั่นแกล้งทางไซเบอร์มากที่สุด นอกจากนั้นผลการสำรวจยังพบว่า เยาวชนไทย อายุ 13 ปีขึ้นไป ร้อยละ 48 เคยเกี่ยวข้องกับการกลั่นแกล้งผ่านทางไซเบอร์ และร้อยละ 41 ของเยาวชนไทยเคยมีประสบการณ์ในการเป็นผู้ถูกกลั่นแกล้งในพื้นที่ไซเบอร์เช่นกัน โดยรูปแบบที่มีการกลั่นแกล้งกันมากที่สุด คือ การนินทาผ่านช่องทางสื่อสารสังคม ส่วนสาเหตุในการกลั่นแกล้งกันมักมาจากการมีกรณีพิพาทกันมาก่อนในพื้นที่จริง และส่วนหนึ่งมากจากการเข้าถึงเทคโนโลยีที่ง่ายและเอื้อให้เกิดกระทำการดังกล่าว (Weerawit Lertratthamrongkul, 2021) ทั้งนี้ สอดคล้องกับผลการวิจัยของ ยูเดส และคณะ (Yudes, Rey, & Extremera, 2022) ที่ได้ระบุว่า การกลั่นแกล้งทางไซเบอร์มักมาจากเหตุของการใช้อินเทอร์เน็ตที่ผิดพลาด (Problematic Internet use) อันมาจากการขาดการควบคุมเวลาผู้เรียนหรือเยาวชนในการเข้าถึงแหล่งข้อมูล หรือกิจกรรมต่าง ๆ ในเครือข่าย จนทำให้ผู้เรียนได้มีโอกาสในการกระทำบางอย่างที่ไม่เหมาะสมได้

2. การสวมรอยหรือการปลอมแปลงทางดิจิทัล (Digital Impersonation) เป็นภัยทางไซเบอร์ที่เกิดขึ้นเป็นจำนวนมากโดยหมายถึงการบุคคลอื่นได้ปลอมตัวตนลงบัญชีช่องทางสื่อสารทางสังคมเพื่อให้เป็นเสมือนเป็นบุคคลนั้นจริง ๆ โดยส่วนมากจะเป็นปลอมบัญชีของบุคคลที่มีชื่อเสียงหรือมีฐานะทางสังคมที่ดีเพื่อต้องการให้ผู้อื่นเกิดความเชื่อถืออันจะนำไปสู่การทำกิจกรรมต่าง ๆ ได้ต่อไป เช่น การหลอกเอาข้อมูลส่วนตัว การโอนเงิน หรือแม้แต่การล่อลวงให้ไปพบเจอเพื่อทำร้ายหรือล่วงละเมิดต่าง ๆ เป็นต้น

จุดเด่นสำคัญของการปลอมแปลงทางดิจิทัล คือ ผู้ที่ทำการสวมรอยหรือปลอมแปลงบุคคลนั้นจะทำการโจรกรรมข้อมูลแทบทุกอย่างของคนที่ถูกปลอมบัญชีมาใช้ เช่น รูปภาพ สถานที่หรือแม้แต่กิจกรรมที่ทำในแต่ละวันเพื่อเป็นการทำให้ผู้อื่นเกิดความเชื่อใจให้ได้มากที่สุด แต่สำหรับในการเรียนการสอน การปลอมแปลงทางดิจิทัลที่เป็นปัญหาในกลุ่มผู้เรียนนั้นจะแบ่งออกได้เป็น 3 ประเภทดังนี้

2.1 การปลอมแปลงบัญชีส่วนตัว (Personal Account Impersonation) เป็นการปลอมแปลงของบัญชีของบุคคลที่มีชื่อเสียง โดยลอกเลียนแบบข้อมูลของบุคคลนั้นเกือบทุกอย่างลงในบัญชีใหม่ที่ทำขึ้นมาเพื่อเป้าหมายในการหลอกลวงเพื่อหวังผลประโยชน์ทางการเงินหรือเพิ่มยอดการติดตาม (Followers) สำหรับการปลอมแปลงบุคคลทางดิจิทัลที่เกี่ยวข้องกับผู้เรียน ส่วนมากจะเป็นการปลอมแปลงบัญชีเป็นผู้อื่นเพื่อการกลั่นแกล้งทางไซเบอร์ไม่ว่าจะเป็นการปล่อยข้อมูลเท็จเพื่อสร้างความสับสน หรือการนินทาว่าร้ายกับผู้เรียนท่านอื่น เป็นต้น

2.2 การยึดครองบัญชีสื่อสารสังคม (Social Media Account Hijacking) เป็นการยึดครองการเข้าสู่ระบบของบัญชีช่องทางการสื่อสารสังคมของบุคคลอื่นโดยไม่ได้ยินยอม ส่วนมากจะเป็นบัญชีทาง Facebook, YouTube หรือ Instagram โดยเจ้าของบัญชีจะไม่สามารถเข้าสู่ระบบบัญชีของตนเองได้อีกต่อไป สำหรับผู้เรียนนั้น การยึดครองบัญชีสื่อสารทางสังคมนี้จะมีเป้าหมายเพื่อการกลั่นแกล้งทางไซเบอร์และการทำกิจกรรมที่เกี่ยวข้องกับคนจำนวนมาก เช่น การเผยแพร่ข่าวสารเป็นเท็จ การขโมยข้อมูลส่วนตัวหรือการสร้างพฤติกรรมที่ไม่เหมาะสมของเจ้าของบัญชีเดิม เป็นต้น

2.3 ปลอมบัญชีบุคคล (Fake Accounts or Bots) เป็นการสร้างบัญชีปลอมขึ้นมาที่ทำงานโดยระบบหรือหุ่นยนต์ (Bot) เพื่อประชาสัมพันธ์ข่าวสาร การส่งข้อความอัตโนมัติ หรือการเข้าถึงกลุ่มต่าง ๆ โดยบัญชีช่องทางสื่อสารสังคมเหล่านี้จะที่ไม่มีบุคคลจริงในการกระทำกิจกรรมดังกล่าว แต่เป็นระบบ

คอมพิวเตอร์ที่ทำกิจกรรมเหล่านั้นเท่านั้น สำหรับผู้เรียนนั้น ภัยอันตรายประเภทนี้เกิดขึ้นเพื่อหวังผลหลอกลวงทางการเงินและการเจาะเอาข้อมูลส่วนตัวเป็นสำคัญ

3. การคัดลอกผลงานทางไซเบอร์ (Cyber Plagiarism) เป็นการคัดลอกผลงานของผู้อื่นมาเป็นของตนเองโดยไม่ได้รับอนุญาต แม้ว่าบทความวิชาการบางส่วนจะเห็นว่าการคัดลอกผลงานทางไซเบอร์นี้จะไม่ได้ถูกจัดอยู่ในภัยอันตรายทางไซเบอร์เท่าไรนัก แต่ก็ถือว่าเป็นอีกหนึ่งปัญหาที่ส่งผลกระทบด้านลบต่อการเรียนการสอนในปัจจุบันที่ควรได้รับการแก้ไขอย่างเร่งด่วน ซึ่ง แอลซารานิ ซาริม และอัมบราฮัม (Alzahrani, Salim, & Abraham, 2012) ได้อธิบายว่า การคัดลอกผลงานทางดิจิทัลนั้นมีหลากหลาย เริ่มต้นด้วยการคัดลอกตัวอักษรหรือเนื้อหาปราศจากการอ้างอิงผลงาน การคัดลอกรูปแบบ ระบบการทำงานต่าง ๆ หรือผลงานที่ปราศจากการอ้างอิงที่ถูกต้อง (Kauffman, & Young, 2015) ซึ่งการคัดลอกนี้ จะนำไปสู่การทำกิจกรรมวิชาการที่ผิดบรรทัดฐาน (Academic Misconduct) ซึ่งถูกพัฒนาต่อไปเป็นการกระทำเรียกว่าการคัดลอกผลงานทางไซเบอร์ (Cyber Plagiarism) ที่มีผลและบทลงโทษตามกฎหมายได้ต่อไป

โอลิเวีย-ดูเมียทริน่า คาสโนว่า และ เคปเดวิล่า (Olivia - Dumitrina, Casanovas, & Capedevilla 2019) ได้อธิบายถึง คัดลอกผลงานทางไซเบอร์ว่าเป็นปัญหาที่มักเกิดขึ้นในกลุ่มผู้เรียนระดับอุดมศึกษามากที่สุด ซึ่งสาเหตุหลักของปัญหาดังกล่าวมาจากการที่ผู้เรียนไม่ทราบว่าการกระทำแบบคัดลอกและวาง (Copy and Paste) นั้นถือว่าเป็นการคัดลอกผลงานทางไซเบอร์ นอกจากนั้น จำนวนผู้เรียนมากกว่าครึ่งหนึ่งเชื่อว่าการแปลภาษา (Translating) ไม่ได้ถือว่าเป็นการคัดลอกผลงานด้วยเช่นกัน ดังนั้นแนวทางการแก้ไขปัญหานี้ คือ การที่ผู้สอนเลือกใช้เครื่องมือในการตรวจสอบการตัดลอกผลงาน รวมไปถึงการส่งเสริมจริยธรรมในการคัดลอกโดยให้ความรู้เรื่องการคัดลอกหรือแนวทางการอ้างอิงผลงาน ซึ่งต่างก็เป็นเนื้อหาส่วนหนึ่งของการส่งเสริมสมรรถนะด้านสื่อและข้อมูลทางดิจิทัลนั่นเอง

จากภัยหรือปัญหาทางไซเบอร์ดังกล่าว จะเห็นได้ว่าสาเหตุของปัญหาเหล่านี้มักมาจากที่ผู้เรียนนั้นขาดการส่งเสริมสมรรถนะทางข้อมูลดิจิทัล (Media information literacy) จนไม่สามารถรู้เท่าทัน หรือคิดวิเคราะห์ในการเลือกเสพและการกระทำการต่อข้อมูลนั้นอย่างเหมาะสม นอกจากนั้น ผู้เรียนยังขาดการส่งเสริมความฉลาดทางดิจิทัล (Digital Intelligence) ที่เอื้อให้ผู้เรียนได้เลือกใช้เครื่องมือหรือแหล่งการข้อมูลเพื่อนำมาสนับสนุนการตัดสินใจในการเลือกเสพข้อมูลได้อย่างงถูกต้อง และท้ายสุดคือ การขาดการส่งเสริมเรื่องความฉลาดทางอารมณ์ (Emotional intelligence) ที่ทำให้ผู้เรียนไม่สามารถควบคุมความคิดของตนเองได้จนทำให้เกิดความแปรปรวนด้านความรู้สึกนึกคิดอันนำไปสู่การแสดงออกทางพฤติกรรมที่ไม่เหมาะสมให้เกิดขึ้นในสังคมไซเบอร์ได้ในที่สุด ซึ่งการขาดเหล่านี้ต่างเป็นหนทางนำไปสู่การถูกกลั่นแกล้ง การถูกหลอกลวงและการกระทำผิดจริยธรรมทางไซเบอร์ได้ในที่สุด

การส่งเสริมความปลอดภัยทางไซเบอร์ต่อผู้เรียน

การสร้างความปลอดภัยทางไซเบอร์สำหรับผู้เรียนนั้น จะแบ่งออกเป็น 2 ส่วนคือ การสร้างสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยแก่ผู้เรียน และการส่งเสริมความรู้ความสามารถที่เกี่ยวข้องกับการสร้างความปลอดภัยทางไซเบอร์ให้เกิดขึ้นภายในตัวผู้เรียน สามารถอธิบายได้ดังนี้

ส่วนที่ 1 สภาพแวดล้อมทางไซเบอร์ที่ปลอดภัย

การสร้างสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยนั้น จำเป็นต้องพิจารณาถึงคุณสมบัติของความปลอดภัยทางไซเบอร์ (CIA Trait) ที่ประกอบไปด้วยคุณสมบัติพื้นฐาน 3 ประการที่สถานศึกษา ผู้สอน และนักการศึกษาควรตระหนักและทำให้เกิดขึ้น เพื่อก่อให้เกิดสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยให้แก่ผู้เรียนได้ โดย ฟาซูโล (Fasulo, 2021) อธิบายคุณสมบัติของสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัย ดังนี้

1. ความมั่นใจ (Confidentiality) สภาพแวดล้อมทางไซเบอร์ปลอดภัยจะต้องประกอบไปด้วยความรู้สึกมั่นใจของผู้ใช้งานในการเข้าถึง เผยแพร่และเก็บรักษาข้อมูลภายในสภาพแวดล้อมทางไซเบอร์นั้น

ดังนั้น การใช้ระบบรักษาความลับของข้อมูลเพื่อเพิ่มความมั่นใจให้แก่ผู้เรียนภายในสภาพแวดล้อมนั้นจึงเป็นสิ่งจำเป็น โดยเฉพาะอย่างยิ่งการลงทุนในการใช้ระบบคัดกรอง ไม่ว่าจะเป็นการใช้โปรแกรมคัดกรองไวรัส ระบบการใส่รหัสผ่าน หรือระบบการเก็บข้อมูลหรือตรวจสอบบุคคลในการเข้าถึงข้อมูลภายในสถานศึกษา เป็นต้น

นอกเหนือจากการลงทุนด้านเครื่องมือแล้ว สถานศึกษาควรออกระเบียบหรือบทลงโทษที่เกี่ยวข้องกับการปลอมแปลงบุคคล การขโมยรหัสผ่านของบัญชีผู้อื่น รวมไปถึงการเผยแพร่ข้อมูลทางไซเบอร์ที่ละเมิดสิทธิ์ของผู้อื่น โดยระเบียบหรือบทลงโทษอาจจะอ้างอิงหรือเกี่ยวข้องกับกฎหมาย PDPA รวมไปถึงส่งเสริมกิจกรรมที่เกี่ยวข้องกับจริยธรรมการสื่อสาร การส่งต่อข่าวหรือหน่วยข่าวกรองต่าง ๆ เป็นต้น

2. ความซื่อสัตย์ สมบูรณ์ (Integrity) สภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยจำเป็นต้องประกอบไปด้วยข้อมูลที่ถูกต้องเพื่อทำให้ผู้เรียนนั้นสามารถเกิดเรียนรู้ได้อย่างมีประสิทธิภาพ รวมไปถึงไม่ตกอยู่ในสภาวะ ไม่ตกอยู่ในภาวะตื่นกลัวหรือมีโอกาสในการตกเป็นเหยื่อจากอาชญากรรมทางไซเบอร์ได้ ซึ่งสถานศึกษาควรเลือกใช้เครื่องมือหรือระบบที่มีการตรวจสอบข้อมูลที่เชื่อมต่อกับฐานข้อมูลภายนอกได้อย่างรวดเร็ว ระบบคัดกรองข้อมูล หรือระบบการรายงานข้อมูลกับหน่วยงานภายนอก นอกจากนั้น สถานศึกษาควรมีหน่วยที่ประกอบไปด้วยบุคคลที่มีหน้าที่ตรวจสอบการเผยแพร่ข้อมูลทางไซเบอร์ รวมไปถึงบุคคลที่มีหน้าที่เกี่ยวข้องกับกฎหมาย เพื่อเป็นการช่วยเหลือให้เกิดการเผยแพร่ข้อมูลที่ถูกต้องในสภาพแวดล้อมนั้นต่อไป

3. ความพร้อม (Availability) สภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยจะต้องประกอบไปด้วยข้อมูลที่หลากหลายและเพียงพอต่อความต้องการของผู้เรียน รวมไปถึงความต่อเนื่องในการใช้ข้อมูลและการให้บริการข้อมูลในสภาพแวดล้อมด้วย ซึ่งสถาบันการศึกษาควรส่งเสริมความพร้อมนี้โดยเลือกใช้เครื่องมือที่มีการจัดการข้อมูลดิจิทัลที่มีความเสถียร ระบบการเชื่อมต่อที่มีประสิทธิภาพ เช่น ระบบปฏิบัติการหลังบ้านที่สามารถจัดการข้อมูลต่าง ๆ หน่วยความจำที่เพียงพอในการเก็บข้อมูล หรือระบบไซเบอร์ที่มีความเสถียรในการกระจายสัญญาณเครือข่าย เป็นต้น

ส่วนที่ 2 ความสามารถด้านความปลอดภัยไซเบอร์ภายในตัวผู้เรียน

จากคุณสมบัติพื้นฐานของสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยข้างต้น สามารถแสดงให้เห็นถึงแนวทางต่อการส่งเสริมความปลอดภัยไซเบอร์ให้เกิดขึ้นภายในตัวผู้เรียนได้เช่นกัน โดยแนวทางที่เกี่ยวข้องกับการสร้างความมั่นใจ ความซื่อสัตย์และความพร้อมนั้นจะเกี่ยวข้องกับความรู้ความสามารถ 3 ด้านที่ผู้เรียนในยุคดิจิทัลควรมีและควรส่งเสริมให้เกิดขึ้น เพื่อเป็นเกราะป้องกันต่อภัยอันตรายทางไซเบอร์ที่อยู่รายล้อมตนเองได้อย่างสมบูรณ์และยั่งยืนได้ต่อไป ซึ่งประกอบไปด้วย

1. ทักษะด้านสื่อและข้อมูลทางดิจิทัล (Media Information Literacy)

ทักษะด้านสื่อและข้อมูลทางดิจิทัล หมายถึงความสามารถของบุคคลในการตรวจสอบ วิเคราะห์แยกแยะข้อมูลที่อยู่ในแหล่งข้อมูลใดก็ตามว่ามีความน่าเชื่อถือได้มากน้อยแค่ไหน รวมไปถึงประเภทของข้อมูลนั้นว่าเป็นข้อมูลที่เกิดขึ้นจริง (Fact) หรือเป็นข้อมูลที่เป็นความคิดเห็นเท่านั้น (Opinion) นอกจากนั้นสมรรถนะด้านนี้ยังมีความหมายครอบคลุมไปถึงการรู้เท่าทันสื่อ นั่นคือความสามารถของบุคคลในการพิจารณาข้อมูลภายในสื่อว่าใครเป็นผู้สร้าง แหล่งข้อมูลนั้นมาจากไหน ข้อมูลนั้นมีคุณค่าหรือมีความเกี่ยวข้องกับตนเองอย่างไร และข้อมูลนั้นได้เผยแพร่ผ่านทางช่องทางที่น่าเชื่อถือมากน้อยเพียงใด (USAID, 2022)

เมื่อผู้เรียนจำเป็นต้องเข้าถึงข้อมูลผ่านทางไซเบอร์ จึงทำให้ความสามารถด้านนี้ความสำคัญมากขึ้น ดังนั้น จะเห็นได้ว่าระบบการศึกษาทั่วโลกต่างได้บูรณาความรู้ความสามารถด้านสื่อและข้อมูลทางดิจิทัลให้เป็นส่วนหนึ่งในรายวิชาหลักที่จำเป็นต้องส่งเสริมให้เกิดแก่ผู้เรียนทุกคน สำหรับประเทศไทยนั้น สมรรถนะด้านสื่อและข้อมูลทางดิจิทัลเป็นหนึ่งในความสามารถที่ควรส่งเสริมให้แก่ประชาชนทุกคนตามแผนกำลังเศรษฐกิจของประเทศ ซึ่งจะเป็นส่วนหนึ่งของมาตราฐานการเรียนรู้ของผู้เรียนในการศึกษาขั้นพื้นฐานของประเทศต่อไป

การส่งเสริมความรู้ความสามารถด้านนี้ ทางองค์การเพื่อการพัฒนาระหว่างประเทศของสหรัฐอเมริกา (U.S. Agency for International Development (USAID), 2022) ได้ร่วมกับองค์กรระดับนานาชาติเอเชียตะวันออกเฉียงใต้ (Association of Southeast Asian Nation: ASEAN) ได้พัฒนาหลักสูตรส่งเสริมทักษะการเข้าถึงข้อมูลและสมรรถนะด้านสื่อดิจิทัล ซึ่งทางองค์กรเองก้ได้สนับสนุนให้สถานศึกษาสามารถนำหลักสูตรนี้ไปปรับใช้ในการสอนในรายวิชาหลักของการศึกษาในทุกระดับ หรือการอบรมแก่บุคลากรทางการศึกษาได้โดยไม่เสียค่าใช้จ่าย โดยเนื้อหาของหลักสูตรนี้จะประกอบไปด้วยเนื้อหาและกิจกรรม 6 ด้านสำคัญที่ช่วยให้ผู้เรียนมีความสามารถในการรู้เท่าทันสื่อดิจิทัลได้อย่างมีประสิทธิภาพ ดังนี้

1. ความรู้พื้นฐานเกี่ยวกับข้อมูลและพลังของข้อมูล (Power of Information) เป็นเนื้อหาที่ส่งเสริมให้ผู้เรียนเกิดความเข้าใจความแตกต่างในข้อมูลแต่ละประเภท และเป้าหมายในการสื่อสารแลกเปลี่ยนข้อมูลในสภาพแวดล้อมทางไซเบอร์ เพื่อให้ผู้เรียนได้รับรู้ถึงอิทธิพลของข้อมูลแต่ละประเภทที่มีต่อจิตใจของบุคคล รวมไปถึงแนวทางในการตรวจสอบข้อมูลทางไซเบอร์ เช่น โปรแกรมในการตรวจสอบ หน่วยงานที่รับผิดชอบในการตรวจสอบข้อมูล เป็นต้น เป็นพื้นฐานสำคัญของการสร้างความตระหนักในความสำคัญของข้อมูลในสภาพแวดล้อมทางไซเบอร์ที่มีต่อผู้เรียนในปัจจุบัน

2. ยุคของข้อมูลเท็จ (The Age of Disinformation) เป็นเนื้อหาที่เน้นถึงการพัฒนาการของรูปแบบข้อมูลเท็จที่ประกอบไปด้วยคุณลักษณะต่าง ๆ รวมไปถึงเป้าหมายและผลกระทบของการสร้างข้อมูลเท็จในสภาพแวดล้อมทางไซเบอร์ พร้อมตัวอย่างประกอบที่เกิดขึ้นจริง ทั้งนี้เพื่อให้ผู้เรียนได้ทราบถึงประเภท ปัญหาและผลกระทบที่เกิดขึ้นจากการเสพหรือส่งต่อข้อมูลเท็จในสภาพแวดล้อมทางไซเบอร์อันเป็นพื้นฐานและแนวทางในการวิเคราะห์ข้อมูลเท็จทางไซเบอร์แก่ผู้เรียนได้ต่อไป

3. การเผยแพร่ข้อมูลอันเป็นเท็จ (How Disinformation Spreads) เนื้อหาเน้นไปที่การอธิบายเทคนิควิธีการและเป้าหมายในการเผยแพร่ข้อมูลอันเป็นเท็จในสภาพแวดล้อมทางไซเบอร์ เพื่อให้ผู้เรียนได้ทราบถึงวิธีการตรวจสอบแหล่งที่มาของข้อมูลเท็จได้ง่ายขึ้น นอกจากนั้น เนื้อหายังเน้นไปที่ความเข้าใจในระบบการทำงานของเครื่องมือ เช่น Algorithms หรือ Filter Bubbles เพื่อช่วยให้ผู้เรียนได้ฝึกคิดวิเคราะห์และตรวจสอบช่องทางในการรับชมสื่อหรือข้อมูลที่ปรากฏในสภาพแวดล้อมไซเบอร์ได้อย่างชัดเจนมากขึ้น

4. แนวโน้มของข้อมูลอันเป็นเท็จ (Recent Trends in Disinformation) เนื้อหาเน้นไปที่ปัญหาและกรณีศึกษาที่เกิดขึ้นจริงเกี่ยวกับการปลอมแปลงข้อมูลที่เกิดขึ้นในสภาพแวดล้อมทางไซเบอร์ในปัจจุบัน และคุณลักษณะของการบิดเบือนข้อมูลผ่านการใช้เทคโนโลยีขั้นสูง (Deep Fake) ที่ปรากฏในสภาพแวดล้อมทางไซเบอร์ เพื่อให้ผู้เรียนได้ทราบถึงเครื่องมือและเตรียมการเฝ้าระวังในการเสพข่างสาวต่างๆผ่านช่องทางไซเบอร์

5. สำนักข่าว สื่อยุคใหม่และข้อมูลอันเป็นเท็จ (Journalists, New Media, and Disinformation) เป็นหัวข้อที่ประกอบไปด้วยเนื้อหาและกิจกรรมที่ส่งเสริมให้ผู้เรียนได้ทราบถึงแหล่งข้อมูลที่มีความน่าเชื่อถือ การส่งเสริมให้รู้แนวทางการตรวจสอบแหล่งข้อมูลและการวิเคราะห์ความถูกต้องของแหล่งข้อมูลนั้น และการทบทวนบทบาทของสำนักข่าวต่อช่องทางการสื่อสารทางไซเบอร์ในปัจจุบันที่อาจจะหายไป หรือหลงลืมไปในองค์กรข่าวหรือหน่วยงานที่เกี่ยวข้องกับการประชาสัมพันธ์ด้านข่าวสาร

6. นักตรวจสอบข้อมูล (Becoming a Disinformation Detective) เป็นหัวข้อที่ประกอบไปด้วยเนื้อหารวบรวมข้อมูลเกี่ยวกับเครื่องมือที่นำมาใช้ในการตรวจสอบแหล่งที่มาของข้อมูล แนวทางในการตรวจสอบข้อเท็จจริงของข้อมูลที่ปรากฏในสภาพแวดล้อมทางไซเบอร์ และข้อมูลด้านกฎหมายี่เกี่ยวข้อง เช่น กฎมาย Copyright หน่วยงานตรวจสอบข่าวกรอง และสนำนักงานตำรวจไซเบอร์ เป็นต้น

2. การส่งเสริมความฉลาดทางดิจิทัล (Digital Intelligence)

ไมทราส และแม็คฟาเรน (Mithas, & McFarlan, 2017) ได้อธิบายความหมายของความฉลาดทางดิจิทัลว่า เป็นความสามารถของบุคคลในการใช้ประโยชน์ของเทคโนโลยีต่อการทำธุรกรรมต่าง ๆ ต่อการดำรงชีวิตได้อย่างประสบความสำเร็จมากที่สุด ทั้งนี้ ความฉลาดทางดิจิทัลแบ่งออกเป็น 3 ระดับ ประกอบไปด้วย

ระดับพื้นฐาน คือ พลเมืองดิจิทัล (Digital citizenship) ที่หมายถึงความสามารถในการใช้เครื่องมือดิจิทัลที่ปลอดภัยและมีประสิทธิภาพเพื่อการดำเนินชีวิตและการงานอาชีพที่เป็นสุข ถือว่าเป็นความฉลาดทางดิจิทัลพื้นฐานที่พลเมืองทุกคนควรมีและสามารถทำได้ไม่ว่าจะเป็นในช่วงอายุใดก็ตาม ระดับต่อมา คือ ความคิดสร้างสรรค์ทางดิจิทัล (Digital creativity) ที่เป็นระดับที่สูงขึ้นจากความสามารถขั้นพื้นฐาน นั่นคือ การที่บุคคลสามารถนำเอาตนเองเข้ามาเป็นส่วนหนึ่งของระบบหรือสภาพแวดล้อมดิจิทัลได้ ผ่านการสร้างสรรค์เนื้อหาหรือองค์ความรู้ใหม่ที่จะนำไปพัฒนาต่อยอดและเห็นผลเชิงประจักษ์ได้ในชีวิตจริงผ่านการใช้เครื่องมือดิจิทัล เป็นระดับความสามารถที่ควรส่งเสริมและพัฒนาให้เกิดขึ้นแก่ผู้เรียนยุคใหม่เป็นสำคัญ และระดับความฉลาดทางดิจิทัลสูงสุดก็คือ การประกอบการดิจิทัล (Digital entrepreneurship) ที่หมายถึงความสามารถของบุคคลในการใช้เครื่องมือดิจิทัลเพื่อแก้ปัญหาในระดับสากล รวมไปถึงการสร้างโอกาสและความท้าทายใหม่ ๆ ให้เกิดขึ้นในสังคมผ่านการใช้เครื่องมือดิจิทัล โดยเป็นความสามารถที่ควรส่งเสริมอย่างต่อเนื่องให้เกิดขึ้นแก่ผู้เรียนในปัจจุบันและอนาคต

วัตสาตรี ดิถียนต์ (Watsatree Diteeyont, 2023) ได้อธิบาความสามารถ 8 ด้านที่ผู้สอนควรส่งเสริมให้เกิดขึ้นเพื่อภายในตัวผู้เรียนเพื่อส่งเสริมให้เกิดความฉลาดทางดิจิทัลได้อย่างประสบความสำเร็จ ซึ่งความสามารถเหล่านั้นประกอบไปด้วย

1. ความสามารถด้านตัวตนดิจิทัล (Digital citizen's identity) ที่หมายถึง การที่ผู้เรียนนั้นสามารถยืนยันตัวตนและบริหารตัวเองได้อย่างเหมาะสมในสภาพแวดล้อมไซเบอร์ ซึ่งการได้มาของความสามารถนี้คือ การที่ผู้สอนจำเป็นต้องส่งเสริมความรู้ความสามารถด้านการสื่อสารทางไซเบอร์ เช่น การใช้เครื่องมือต่าง ๆ การใช้ภาษา และสถานการณ์ในการสื่อสารที่เหมาะสม นอกจากนั้น ยังควรส่งเสริมให้ผู้เรียนได้ทราบแนวทางการเผยแพร่และรักษาข้อมูลส่วนตัวในสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัย เช่น การไม่เผยแพร่ข้อมูลส่วนตัวในพื้นที่สาธารณะ การสร้างและรักษารหัสผ่านที่เหมาะสม เป็นต้น

2. การจัดการการกลั่นแกล้งในไซเบอร์ (Cyberbullying management) เป็นความสามารถของผู้เรียนในการระบุคุณลักษณะของสถานการณ์ที่เลวร้ายหรือสถานการณ์ที่ขัดแย้งกันภายในสภาพแวดล้อมทางไซเบอร์และสามารถจัดการและควบคุมสถานการณ์นั้นได้เป็นอย่างดี โดยผู้สอนควรส่งเสริมให้ผู้เรียนรู้จักประเภทของภัยคุกคามที่เกิดขึ้น รวมไปถึงระดับความรุนแรงและแนวทางการจัดการปัญหาที่เหมาะสม เช่น การรายงานปัญหาให้ครูหรือครอบครัวทราบ หรือการขอความช่วยเหลือจากหน่วยงานที่ปกป้องภัยคุกคามทางไซเบอร์ เป็นต้น นอกจากนั้น รวมไปถึงการจัดการและควบคุมอารมณ์ของตนเองในการแสดงออกทางไซเบอร์ที่จำเป็นต้องฝึกฝนการรู้เท่าทันตนเองเป็นสำคัญ

3. การจัดการข้อมูลส่วนตัว (Privacy management) เป็นความสามารถของผู้เรียนในการจัดการและเผยแพร่ข้อมูลส่วนตัวลงในสภาพแวดล้อมทางไซเบอร์ได้อย่างปลอดภัย โดยจะต้องอยู่ภายใต้ขอบเขตของการปกป้องข้อมูลในความเป็นส่วนตัวได้ ซึ่งความสามารถในการจัดการข้อมูลส่วนตัวนี้ ผู้สอนควรสนับสนุนให้ผู้เรียนได้ทราบประเภทและลักษณะของข้อมูลที่เหมาะสมและไม่เหมาะสมต่อการเผยแพร่ทางไซเบอร์ รวมไปถึงการศึกษากรณีศึกษาและส่งเสริมประสบการณ์การแก้ปัญหาและการป้องกันการโจรกรรมข้อมูลทางไซเบอร์

4. ลายนิ้วมือดิจิทัล (Digital Fingerprint) เป็นความสามารถของผู้เรียนในการเข้าใจและยอมรับผลของการกระทำที่เกิดขึ้นในสภาพแวดล้อมทางไซเบอร์ที่อาจจะส่งผลต่อการดำรงอยู่ในชีวิตจริงของตนเองได้ต่อไป การส่งเสริมความสามารถด้านนี้สามารถได้โดย ผู้สอนควรส่งเสริมให้ผู้เรียนได้ทราบผลกระทบของการกระทำกิจกรรมต่าง ๆ ในสภาพแวดล้อมทางไซเบอร์ที่อาจจะส่งผลต่อสังคมและตัวเองในอนาคตผ่านกรณีศึกษาที่เกิดขึ้นจริง เช่น ผลจากการที่เคยเผยแพร่ภาพส่วนตัว การแสดงออกทางความคิดในช่องทางสังคมของบุคคลต่าง ๆ เป็นต้น นอกจากนั้น ผู้สอนยังควรส่งเสริมให้ผู้เรียนได้ทราบแนวทางสำหรับการจัดการและประสบการณ์ในการแก้ไขปัญหาเหล่านั้นอย่างมีประสิทธิภาพ

5. การจัดการเวลาหน้าจอ (Screen time management) หมายถึงความสามารถในการเฝ้าระวังและตรวจสอบตนเองในการบริหารจัดการเรื่องเวลาในการทำกิจกรรมทางไซเบอร์อย่างเหมาะสม ไม่ว่าจะเป็นการเล่นเกมออนไลน์ การติดต่อสื่อสารผ่านช่องทางการสื่อสารสังคม หรือการเข้าถึงแหล่งข้อมูลทางไซเบอร์ต่าง ๆ โดยผู้สอนควรส่งเสริมให้ผู้เรียนได้เรียนรู้ผลกระทบด้านร่างกายและจิตใจจากการใช้เทคโนโลยีมาจนเกินไป เช่น การป่วยเป็นโรคออฟฟิศซินโดรม โรคทางสายตา หรือแม้แต่สุขภาพจิตที่หมกหมุ่นในการเสพข่าวสารมากจนเกินไป เป็นต้น

6. การจัดการความปลอดภัยทางไซเบอร์ (Cybersecurity management) หมายถึง ความสามารถของผู้เรียนในการบริหารจัดการภัยที่เกิดขึ้นในเครือข่ายและผู้เรียนสามารถปกป้องข้อมูลของตนเองได้ โดยผู้สอนควรสนับสนุนให้ผู้เรียนได้มีความรู้พื้นฐานเรื่องเครื่องมือที่นำมาใช้เพื่อป้องกันการโจรกกรรมข้อมูล ระบบการจัดการบัญชีทางช่องทางสังคม เช่น โปรแกรมป้องกันไวรัสคอมพิวเตอร์ แนวทางการตั้งรหัสผ่านของบัญชี หรือการเปลี่ยนรหัสผ่าน อย่างสม่ำเสมอ นอกจากนั้น ผู้สอนควรให้ความรู้เรื่องประเภทของภัยคุกคามที่เกิดขึ้นในสภาพแวดล้อมไซเบอร์ และแนวทางการป้องกันภัยเหล่านั้นได้ด้วยตนเอง เช่น การงดเผยแพร่ข้อมูลส่วนตัว การเก็บข้อมูลการคุกคามเพื่อเอาผิดทางกฎหมาย หรือการรายงานหน่วยงานที่เกี่ยวข้อง เป็นต้น

7. การคิดวิเคราะห์ (Critical thinking) เป็นความสามารถของผู้เรียนในการแบ่งแยกข้อมูลถูกผิด ข้อมูลทางบวกหรือลบ ข้อมูลที่มีความน่าเชื่อถือ หรือการระบุถึงบุคคลที่ไม่ทราบที่มาที่ไป โดยผู้สอนควรสนับสนุนให้ผู้เรียนได้ฝึกการคิดวิเคราะห์ข้อมูลเพื่อเปรียบเทียบความแตกต่างและค้นหาที่มาของข้อมูลในไซเบอร์เหล่านั้นว่ามีความถูกต้องและน่าเชื่อถือมากน้อยเพียงใด เช่น การฝึกการตั้งคำถาม การฝึกค้นหาข้อมูล การฝึกเปรียบเทียบและหาความเชื่อมโยงของข้อมูล เป็นต้น

8. ความเข้าใจทางดิจิทัล (Digital empathy) เป็นความสามารถของผู้เรียนในการเข้าใจความต้องการ อารมณ์และความรู้สึกของทั้งตนเองและผู้อื่นภายในสภาพแวดล้อมทางไซเบอร์ โดยผู้สอนควรสนับสนุนให้ผู้เรียนได้แลกเปลี่ยนเรียนรู้เพื่อให้ทราบมุมมองที่หลากหลาย ฝึกการควบคุมอารมณ์เพื่อให้เกิดการรู้เท่าทันตนเองและฝึกการบริหารจัดการอารมณ์ของตนเองเพื่อเป็นพื้นฐานในการสร้างความฉลาดทางอารมณ์ได้ต่อไป

3. การส่งเสริมความฉลาดทางอารมณ์ (Emotional Intelligence)

ความฉลาดทางอารมณ์มีความหมายถึง การที่บุคคลนั้นสามารถเข้าใจ ควบคุมและใช้ความคิดและความรู้สึกของตนเองได้อย่างเหมาะสม ซึ่งจะนำไปสู่การแสดงออกทางพฤติกรรมที่ดีและก่อให้เกิดประโยชน์แก่ตนเองได้ต่อไป นอกจากนั้น ความฉลาดทางอารมณ์ยังมีความหมายถึงความสามารถในการรับรู้ความรู้สึกของตนเองและผู้อื่น รวมไปถึงการกระทำหรือแสดงออกในการรักษาความสัมพันธ์ระหว่างบุคคลนั้นให้ดำเนินต่อไปได้ต่อไปอย่างราบรื่น (Mayer, 2017)

สำหรับการเรียนการสอน ความฉลาดทางอารมณ์จะช่วยให้ผู้เรียนสามารถสื่อสารผ่านทางไซเบอร์ได้อย่างปลอดภัยและไม่ส่งผลกระทบด้านลบต่อตนเองและผู้อื่น อันเป็นปัจจัยที่ทำให้ผู้เรียนประสบความสำเร็จทางการเรียนได้มากขึ้น (Mohzan, Hassan, & AbdHalil, 2013) เพราะผู้เรียนที่มีความฉลาดทางอารมณ์นั้นจะสามารถจัดการความกดดันในการเรียนได้ดี (Enns, Eldridge, Montgomery, & Gonzalez, 2018) ทั้งนี้ โกลแมน (Goleman, 1995) ได้อธิบายเพิ่มเติมว่า ความฉลาดทางอารมณ์นั้นเกี่ยวข้องกับความสามารถในพุทธพิสัยของบุคคล ดังนั้น การพัฒนาหรือส่งเสริมความฉลาดทางอารมณ์นี้จึงจำเป็นต้องส่งเสริมความสามารถทางการคิดเป็นสำคัญ โดย โกลแมน (Goleman, 2001 as cited in Kanesan, & Fauzan, 2019) ได้สรุปแนวทางการส่งเสริมความฉลาดทางอารมณ์ ซึ่งประกอบไปด้วย 2 ส่วนสำคัญ คือ ส่วนในการพัฒนาตนเอง (Personal Competence) และส่วนในการพัฒนาทางสังคม (Social Competence) โดยแต่ละส่วนจะแบ่งออกเป็น 2 ส่วนย่อยที่ประกอบ ไปด้วยการรับรู้และการควบคุม สามารถอธิบายได้ดังนี้

ส่วนที่ 1. การพัฒนาตนเอง (Personal Competence) การพัฒนาตนเองเพื่อส่งเสริมความฉลาดทางอารมณ์นั้น จะแบ่งออกเป็น 2 ส่วนย่อย คือ

1.1 ด้านการรับรู้ (Recognition) ที่ประกอบไปด้วย การส่งเสริมความตระหนักรู้ด้วยตนเอง (Self - Awareness) ที่หมายถึง ความสามารถในการรู้เท่าทันตนเอง ไม่ว่าจะเป็นความรู้สึกนึกคิด รวมไปถึงจุดเด่นและจุดด้อยของตนเอง เพื่อเป็นพื้นฐานต่อการนำไปสู่การตัดสินใจในการกระทำหรือการแสดงออกของตนเองได้ต่อไป ซึ่งการส่งเสริมการตระหนักรู้นี้ ผู้สอนควรสนับสนุนให้ผู้เรียนได้มีโอกาสในการตรวจสอบความรู้สึกของตนเอง ไม่ว่าจะเป็นการจดบันทึก หรือการแลกเปลี่ยนเรียนรู้ เพื่อให้ผู้เรียนได้ทบทวนตนเองว่า สิ่งที่ได้รับรู้มาคืออะไร รู้สึกอย่างไร และเพราะอะไรจึงเกิดความรู้สึกหรือทัศนคติเช่นนั้น

1.2 การควบคุม (Regulation) ผู้เรียนที่สามารถควบคุมตนเองได้มักมาจากการที่ผู้เรียนได้รู้จักการรู้เท่าทันตนเอง ดังนั้น การควบคุมจึงเป็นส่วนที่เน้นเรื่อง การบริหารตนเอง (Self - Management) หมายถึง ความสามารถในการบริหารจัดการและควบคุมการแสดงออกของผู้เรียนจากอารมณ์ความรู้สึกในตอนนั้นโดยผู้สอนควรให้ผู้เรียนได้เรียนรู้และฝึกปฏิบัติในเรื่องการแสดงออกทางความคิดเห็นที่เหมาะสมภายในไซเบอร์ผ่านการเรียนรู้จากกรณีศึกษา หรือฝึกฝนสมาธิเพื่อให้เกิดสติและความสามารถในการคิดวิเคราะห์ถึงผลได้ผลเสียของการแสดงออกทางอารมณ์นั้นออกไป

ส่วนที่ 2 การพัฒนาทางสังคม (Social Competence) การพัฒนาทางสังคมเพื่อส่งเสริมความฉลาดทางอารมณ์นั้นจะแบ่งออกเป็น 2 ส่วนย่อยเช่นกัน ประกอบไปด้วย

2.1 การรับรู้ (Recognition) การรับรู้ในส่วนนี้จะเน้นเรื่อง ความตระหนักรู้ทางสังคม (Social Awareness) ที่หมายถึงเป็นความสามารถของผู้เรียนในการทราบมุมมองและความคิดเห็นของผู้อื่น การบริการหรือการตอบสนองต่อสังคม หรือแนวความคิดที่เป็นประเด็นสำคัญทางสังคม ซึ่งผู้เรียนที่มีการรับรู้การรับรู้ในด้านนี้จะช่วยให้ผู้เรียนได้ทราบมุมมองที่แตกต่าง อันนำไปสู่การคิดวิเคราะห์เพื่อหาแนวทางการแสดงออกได้อย่างเหมาะสมต่อไป โดยผู้สอนควรสนับสนุนให้ผู้เรียนแสดงบทบาทสมมุติ (Play role) ในสถานการณ์ที่กำหนดเพื่อที่จะได้รับรู้ความรู้สึกในแต่ด้านหรือบทบาทที่ได้รับ หรือการแลกเปลี่ยนเรียนรู้ระหว่างผู้เรียน หรือแหล่งการเรียนรู้ที่หลากหลายเพื่อให้เกิดการรับรู้ความคิดเห็นที่หลากหลายในประเด็น

2.2 การควบคุม (Regulation) การควบคุมในส่วนของพัฒนาสังคมจะประกอบไปด้วย การบริหารจัดการความสัมพันธ์ (Relationship Management) ที่หมายถึงความสามารถของผู้เรียนในการสื่อสาร การจัดการความขัดแย้ง การทำงานร่วมกันและการแก้ไขปัญหา โดยผู้เรียนที่สามารถบริหารจัดการความสัมพันธ์ได้จะสามารถรักษาความสัมพันธ์หรือการสื่อสารนั้นให้ดำรงอยู่หรือดำเนินต่อไปได้อย่างราบรื่น รวมไปถึงการทำกิจกรรมการเรียน การแสดงความคิดเห็นหรือการทำกิจกรรมกลุ่มที่ประสบความสำเร็จ อีกทั้งยังเป็นพื้นฐานสำคัญของการสร้างสภาพแวดล้อมการเรียนรู้ที่ดีและมีแรงจูงใจในการเรียนที่เพิ่มมากขึ้นได้ ดังนั้น ผู้สอนควรเปิดโอกาสให้ผู้เรียนได้ฝึกฝนการจัดการปัญหาจากกรณีศึกษาต่าง ๆ เพื่อให้ผู้เรียนได้มีประสบการณ์อย่างเพียงพอและสามารถจัดการบริการปัญหาเหล่านั้นได้อย่างมีประสิทธิภาพเมื่อสถานการณ์จริงเข้ามาถึง

บทสรุป

การเรียนการสอนในปัจจุบันถือว่าเป็นรูปแบบการเรียนรู้ที่เอื้อให้ผู้เรียนได้มีโอกาสในการเข้าถึงแหล่งข้อมูลที่มีอยู่อย่างมากมายผ่านการเชื่อมต่อทางไซเบอร์ได้อย่างไร้ข้อจำกัด ดังนั้น จึงเป็นเหตุให้การสร้างความปลอดภัยทางไซเบอร์ (Cyber Security Competency) ได้กลายเป็นประเด็นสำคัญที่ควรได้รับการส่งเสริมแก่ผู้เรียนในการเรียนการสอนยุคดิจิทัลอย่างเร่งด่วน โดยการส่งเสริมความปลอดภัยทางไซเบอร์ได้แบ่งออกเป็น 2 ด้านคือ การสร้างสภาพแวดล้อมที่ปลอดภัยและความรู้ความสามารถที่เกี่ยวข้องให้เกิดขึ้นภายในตัวผู้เรียน ซึ่งประกอบไปด้วยความรู้ความสามารถในการเข้าถึง ตรวจสอบ วิเคราะห์ แยกแยะข้อมูลที่อยู่ในแหล่งข้อมูลว่ามีความน่าเชื่อถือแค่ไหน รวมไปถึงการส่งเสริมความฉลาดทางดิจิทัลที่ช่วยให้ผู้เรียนได้เข้าใจและการใช้พลังประโยชน์ของเทคโนโลยีต่อการเรียนการสอนให้ได้มากที่สุด และท้ายสุดคือการส่งเสริมความฉลาด

ทางอารมณ์ ที่หมายถึง ความสามารถของผู้เรียนในการจัดการความรู้สึกนึกคิดและการแสดงออกของตนเองได้อย่างเหมาะสมในสภาพแวดล้อมทางไซเบอร์

References

Alzahrani, S. M., Salim, N., & Abraham, A. (2011). Understanding plagiarism linguistic patterns, textual features, and detection methods. *IEEE Transactions on Systems, Man, and Cybernetics, 42*(2), 133 - 149.

Chadwick, S. (2014). Impacts of cyberbullying, building social and emotional resilience in schools. *Springer Science & Business Media, 42*(2), 133 - 149.

Enns, A., Eldridge, G. D., Montgomery, C., & Gonzalez, V. M. (2018). Perceived stress, coping strategies, and emotional intelligence: A cross-sectional study of university students in helping disciplines. *Nurse Educ. Today*, *68*, 226 – 231

Fasulo, P. (2021). *What is the CIA trait? definition, importance, & example*. Retrieved from https://securityscorecard.com/blog/what-is-the-cia-triad/

Goleman, D. (1995). *Emotional intelligence: Why it can matter more than IQ for character health and lifelong achievement*. New York: Bantam Books.

Goleman, D. (2001). An EI-based theory of performance. In C. Cherniss & D. Goleman (Eds.), *The emotionally intelligent workplace: How to select for, measure, and improve emotional intelligence in individuals, groups, and organizations.* San Francisco, CA: Jossey-Bass.

Kanesan, P., & Fauzan, N. (2019). Models of emotional intelligence: A review. *e-Bangi*, *16*, 1 - 9.

Kauffman, Y., & Young, M. F. (2015). Digital plagiarism: An experimental study of the effect of instructional goals and copy-and-paste affordance. *Computers & Education*, *83*, 44 - 56.

Weerawit Lertratthamrongkul. (2021). Cyberbullying among secondary school students: Prevalence, problem - solving and skill behaviors. *NEU Academic and Research Journal, 11*(1), 275 – 289.

Mithas, S., & McFarlan, F. W. (2017). What is digital intelligence? *IT Professional, 19*(4), 3 - 6.

Mayer, J. D. (2017). *Section 1: what is emotional intelligence? HBR guide to emotional intelligence (HBR Guide Series).* Boston: Harvard Business Review Press. Retrieved from https://search-ebscohost.com.ezproxy.snhu.edu/login.aspx?direct=true&db=nlebk&AN=1798590&site=eds-live&scope=sit

Mohzan, M. A. M., Hassan, N., & AbdHalil, N. (2013). The influence of emotional intelligence on academic achievement. *Procedia*, *90*, 303 – 312.

Nixon, C. L. (2014). Current perspectives: The impact of cyberbullying on adolescent health. *Adolescent Health, Medicine and Therapeutics, 5*, 143 - 158.

Olivia-Dumitrina, N., Casanovas, M., & Capdevila, Y. (2019). Academic writing and the internet: Cyber-plagiarism amongst university students. *Journal of New Approaches in Educational Research*, *8*(2), 112 - 125.

Rahman, N. A. A., Sairi, I., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology, 10*(5), 378 - 382.

U.S. Agency for International Development (USAID). (2022). *Disinformation and Promote Media Literacy.* USA: Pilot Training of trainer program.

Watsatree Diteeyont. (2023). *Textbook of Educational technology*. (Unpublished Textbook). Educational Technology Department, Faculty of Education, Kasetsart University.

Weerawit Lertratthamrongkul. (2021). Cyberbullying among Secondary school students: Prevalence, problem - solving and skill behaviors. *NEU Academic and Research Journal, 11*(1), 275 – 289.

Yudes, C., Rey, L., & Extremera, N. (2022). The moderating effect of emotional intelligence on problematic internet use and cyberbullying perpetration among adolescents: Gender differences. *Psychological Reports*, *125*(6), 2902 - 2921.

Received: 2023, March 29
Revised: 2023, June 19
Accepted: 2023, June 21