เทคโนโลยีอัจฉริยะบิดดีเฟนเดอร์ สคามิโอ เพื่อเสริมสร้างความปลอดภัยในโลกไซเบอร์ของผู้เรียนยุคดิจิทัล

BITDEFENDER SCAMIO INTELLIGENT TECHNOLOGY TO ENHANCE CYBERSECURITY FOR DIGITAL ERA LEARNERS

พีรพล แซ่หลี[1] และอุทิศ บำรุงชีพ[2]
Peerapon Saelee[1] and Uthit Bamroongcheep[2]
คณะศึกษาศาสตร์ มหาวิทยาลัยบูรพา
Faculty of Education Burapha University
E-mail: fong.peerapon@hotmail.com

บทคัดย่อ

บทความวิชาการนี้มุ่งศึกษาเทคโนโลยีอัจฉริยะบิดดีเฟนเดอร์ สคามิโอ เป็นโปรแกรมที่สามารถนำมาประยุกต์ใช้ในการเสริมสร้างความปลอดภัยในโลกไซเบอร์ให้กับผู้เรียนยุคดิจิทัลได้ ทั้งนี้เนื่องจากการใช้งานอินเทอร์เน็ตได้ทวีเพิ่มขึ้นอย่างรวดเร็ว การรู้ดิจิทัล การใช้เทคโนโลยีสารสนเทศและการสื่อสารอย่างปลอดภัย การจัดการ การรู้เท่าทันสื่อนวัตกรรมและผลกระทบของเทคโนโลยีสารสนเทศและการสื่อสารต่อการดำเนินชีวิต อาชีพ และสังคม การโจมตีทางไซเบอร์ที่ซับซ้อนและหลากหลายรูปแบบทำให้ผู้ใช้อินเทอร์เน็ตต้องเผชิญกับความเสี่ยงในการถูกหลอกลวงผ่านอีเมล ข้อความ และลิงก์ต่าง ๆ ซึ่งโปรแกรม บิดดีเฟนเดอร์ สคามิโอ ถูกพัฒนาเพื่อช่วยตรวจจับการหลอกลวงออนไลน์โดยใช้ปัญญาประดิษฐ์ (AI) วัตถุประสงค์คือช่วยให้ผู้ใช้สามารถส่งเนื้อหาที่น่าสงสัยสามารถให้โปรแกรมวิเคราะห์และรับคำตอบภายในไม่กี่วินาที ดังนั้นถ้านำบูรณาการในการจัดการเรียนการสอนในตัวชี้วัดที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ สามารถนำไปเป็นกรณีศึกษาโดยการระบุและป้องกันภัยคุกคามที่อาจเกิดขึ้นจากการใช้งานอินเทอร์เน็ต นอกจากนี้ บิดดีเฟนเดอร์ สคามิโอ ไม่เพียงแต่ช่วยในการตรวจจับภัยคุกคาม แต่ยังส่งเสริมให้ผู้เรียนมีความรับผิดชอบและจริยธรรมในการใช้งานเทคโนโลยีดิจิทัล โดยมุ่งหวังให้ผู้เรียนสามารถเรียนรู้และสื่อสารออนไลน์ได้อย่างปลอดภัยในโลกที่เต็มไปด้วยความอันตรายทางไซเบอร์

คำสำคัญ : เทคโนโลยีอัจฉริยะ , บิดดีเฟนเดอร์ สคามิโอ , ความปลอดภัยในโลกไซเบอร์ , ผู้เรียนยุคดิจิทัล

*Received December 3, 2024; Revised December 19, 2024; Accepted January 23, 2025

Abstract

The Bitdefender Scamio intelligent technology is a program that can be applied to enhance cybersecurity for digital-era learners. This is especially important as internet usage has rapidly increased. Digital literacy, the safe use of information and communication technology (ICT), media awareness, and understanding the impacts of ICT on daily life, careers, and society are crucial. The rise of complex and diverse cyberattacks means internet users face the risk of being deceived through emails, messages, and various links. Bitdefender Scamio was developed to help detect online scams using artificial intelligence (AI). The goal is to enable users to submit suspicious content for analysis and receive results within seconds. Therefore, integrating this technology into teaching methods related to cybersecurity can serve as a case study for identifying and preventing potential threats from internet usage. Furthermore, Bitdefender Scamio helps detect threats and promotes responsible and ethical use of digital technology, aiming to ensure learners can safely learn and communicate online in a world full of cyber risks.

Keywords : Intelligent Technology , Bitdefender Scamio, Cybersecurity , Digital Era Learners

บทนำ

มิติของความพลิกผันในโลกไซเบอร์เกิดจากความก้าวกน้าของเทคโนโลยีซึ่งเป็นช่วงเวลาที่เรียกว่า “ยุคดิจิทัล” ซึ่งมีบทบาทสำคัญในชีวิตประจำวัน การเผชิญกับภัยคุกคามทางไซเบอร์ เช่น การหลอกลวงออนไลน์ ได้กลายเป็นปัญหาที่เพิ่มขึ้นอย่างต่อเนื่อง Thaihealth (2024) โดยเฉพาะอย่างยิ่งในช่วงไม่กี่ปีที่ผ่านมา ที่มีการรายงานว่าความสูญเสียจากการหลอกลวงออนไลน์ในปี 2023 มีมูลค่าความเสียหายสูงถึง 50,000 ล้านบาท Khurunun and Saengthongdee (2023) กล่าวว่า การป้องกันและปราบปรามอาชญากรรมไซเบอร์ในยุคปัจจุบันให้มีประสิทธิภาพมากที่สุดคือการสร้างภูมิคุ้มกันให้กับประชาชนให้สามารถที่จะมีความรู้ความเข้าใจและรู้ทันกับมิจฉาชีพที่จะมาติดต่อพูดคุยและใช้ช่องทางออนไลน์ในการเข้ามาก่ออาชญากรรมได้ ส่งผลให้ความก้าวหน้าของเทคโนโลยีมาพร้อมกับอันตรายที่เกิดจากมิจฉาชีพบนโลกออนไลน์ในยุคดิจิทัลที่สามารถเข้าถึงข้อมูลและแพร่กระจายได้อย่างรวดเร็ว ดังนั้นจึงต้องมีมาตรการเพื่อเสริมสร้างความปลอดภัยในโลกไซเบอร์

ความปลอดภัยในโลกไซเบอร์ (Cyber Security) Electronic Transactions Development Agency (2021) คือ วิธีการ มาตรการ หรือการดำเนินการใด ๆ เพื่อป้องกัน รับมือ บรรเทา และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่มีผลต่อปัจจัยการรักษา ความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของอุปกรณ์และข้อมูลภายในระบบสารสนเทศ ซึ่งหากการรักษาความมั่นคง ปลอดภัยทางไซเบอร์มีความอ่อนแออาจทำให้ผู้ประสงค์ร้ายสามารถสร้างความเสียหายต่อตัว ผู้ใช้งานและข้อมูลส่วนบุคคลของผู้ใช้งานได้ Putwattana (2021) โดยเฉพาะอย่างยิ่งความก้าวหน้าทางเทคโนโลยีดิจิทัลที่เข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตของมนุษย์ในทุกๆ ด้าน รวมไปถึง การเรียนรู้ พฤติกรรมและรูปแบบการเรียนรู้ของผู้เรียนจึงเปลี่ยนแปลงไปจากเดิม องค์ความรู้ต่างๆ ไม่ได้จำกัดอยู่เพียงในห้องเรียนอีกต่อไป ผู้เรียนสามารถเข้าถึงแหล่งเรียนรู้ได้หลากหลายมากขึ้น ผู้เรียนในยุคดิจิทัลซึ่งต้องใช้เวลาส่วนใหญ่อยู่กับ

การเรียนรู้ผ่านระบบออนไลน์ จึงมีความเสี่ยงสูงที่จะตกเป็นเหยื่อของภัยคุกคามทางไซเบอร์รูปแบบต่างๆ ไม่ว่าจะเป็นการหลอกลวงผ่านการซื้อสินค้าออนไลน์ หรือการหลอกลวงด้านการลงทุน ซึ่งล้วนส่งผลกระทบทั้งด้านการเงินและสภาพจิตใจ

ผลกระทบจากความก้าวหน้าของเทคโนโลยีดิจิทัลนั้นในวงการศึกษาควรสร้างทักษะให้กับผู้เรียนซึ่งนอกจากสอนให้มีความรู้ ความเข้าใจเพื่อการสร้างภูมิคุ้มกันให้แก่ผู้เรียนในยุคดิจิทัลแล้วนั้นควรเสริมสร้างทักษะให้รู้จักวิธีการป้องกันด้วยซึ่งสอดคล้องกับ Novak (2024) ได้กล่าวว่า การพัฒนาเทคโนโลยีที่สามารถช่วยป้องกันและตรวจจับการหลอกลวงมีความสำคัญอย่างยิ่ง หนึ่งในนวัตกรรมที่น่าสนใจคือ บิดดีเฟนเดอร์ สคามิโอ (Bitdefender Scamio) ซึ่งเป็นแชทบอทที่ใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) ในการตรวจจับการหลอกลวงออนไลน์อย่างรวดเร็ว โดยสามารถวิเคราะห์ลิงก์ ข้อความ อีเมล และ คิวอาร์โค้ด เพื่อช่วยให้ผู้ใช้สามารถป้องกันตนเองจากการหลอกลวงที่มีความซับซ้อน ทั้งนี้รายวิชา เทคโนโลยี (วิทยาการคำนวณ) หลักสูตรการศึกษาขั้นพื้นฐานได้กำหนดตัวชี้วัดให้ผู้เรียนได้ใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย มีจริยธรรม ให้เหมาะสมกับการเปลี่ยนแปลง ดังนั้นบิดดีเฟนเดอร์ สคามิโอ จึงเป็นโปรแกรมหนึ่งที่สามารถนำมาใช้ในการเรียนรู้ให้เกิดทักษะความปลอดภัยในโลกไซเบอร์สำหรับผู้เรียนในยุคดิจิทัลอย่างมีประสิทธิภาพ

จากที่กล่าวมาข้างต้นบทความนี้มีวัตถุประสงค์เพื่อศึกษาและนำเสนอในการใช้เทคโนโลยีปัญญาประดิษฐ์ (AI) บิดดีเฟนเดอร์ สคามิโอ ให้เกิดประโยชน์ในด้านความปลอดภัยในโลกไซเบอร์ โดยเน้นให้ผู้เรียนในยุคดิจิทัลที่หลักสูตรได้กำหนดให้ผู้เรียนได้ศึกษารายวิชาเทคโนโลยี (วิทยาการคำนวณ) ได้เข้าใจถึงความสำคัญของการรักษาความปลอดภัยในโลกไซเบอร์ ตระหนักถึงภัยคุกคามที่อาจเกิดขึ้นจากการใช้งาน โดยมีความรู้และทักษะในการป้องกันตัวเองจากภัยคุกคามทางไซเบอร์ และส่งเสริมให้ผู้เรียนมีความรับผิดชอบและจริยธรรมในการใช้งานเทคโนโลยีดิจิทัล โดยคำนึงถึงความปลอดภัยและการปกป้องข้อมูลส่วนบุคคลตามพลเมืองดิจิทัล และนำไปประยุกต์ใช้ให้เกิดประโยชน์ในชีวิตดิจิทัลต่อไป

เนื้อหา

จากการศึกษาและวิเคราะห์จากเอกสารและงานวิจัยที่เกี่ยวข้อง พบว่า สถานการณ์ภัยคุกคามทางไซเบอร์มีความซับซ้อนและหลากหลายมากยิ่งขึ้น โดยเฉพาะในประเทศไทย สถานการณ์ภัยคุกคามทางไซเบอร์ยังคงเป็นเรื่องที่ต้องให้ความสำคัญอย่างต่อเนื่อง แม้ว่ามีการบังคับใช้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งมุ่งเน้นการสร้างมาตรฐานความปลอดภัยทางไซเบอร์ให้กับองค์กรทั้งภาครัฐและเอกชน แต่ยังคงมีข่าวการโจมตีที่เป็นภัยคุกคามในโลกไซเบอร์ตลอดหลายปีที่ผ่านมาจนถึงปัจจุบัน SOSECURE (2024) ดังตัวอย่างสถานการณ์ต่อไปนี้

1. ตัวอย่างสถานการณ์ในเดือนกุมภาพันธ์ พ.ศ.2565 TCAS ทำข้อมูลส่วนตัวนักเรียนปี 64 รั่วไหลจากเว็บไซต์ mytcas.com จำนวนกว่า 23,000 รายการ มีตั้งแต่ชื่อ-นามสกุล, เลขบัตรประจำตัวประชาชน, โปรแกรมที่สมัครและรอบที่สมัครสอบ

2. ตัวอย่างสถานการณ์ในเดือนมีนาคม พ.ศ.2566 9Near ประกาศขายข้อมูลส่วนตัวคนไทย 55 ล้านคน พร้อมขายเป็นสกุลเงินบิทคอยน์ ข้อมูลหลุดมีแทบจะครบตั้งแต่ชื่อ, ที่อยู่, เลขประจำตัวประชาชน สาเหตุรั่วไหลมาจากหน่วยงานรัฐในไทย

3. ตัวอย่างสถานการณ์ในเดือนพฤศจิกายน พ.ศ.2567 ร้านเครื่องดื่มและอาหารชื่อดัง ทำข้อมูลลูกค้าหลุดมากกว่า 958GB พร้อมแนบลิงก์ภาพหลักฐานถูกขโมยผ่านทางแอปพลิเคชัน LINE

นอกจากนี้ งานวิจัยของ Khurunun and Saengthongdee (2023) พบว่าอาชญากรรมไซเบอร์ที่มีลักษณะคอมพิวเตอร์ตกเป็นเป้าหมายในการกระทำความผิดที่เรียกกันว่า Hacker ซึ่งหมายถึง ผู้ที่ใช้ระบบ

คอมพิวเตอร์เพื่อเข้าถึง ข้อมูล หรือเป็นผู้ที่ทำให้ระบบอื่นไม่พร้อมใช้งานโดยไม่ได้รับอนุญาต และการโจมตีทางไซเบอร์ (Cyber Attack) โดยใช้คอมพิวเตอร์หนึ่งเครื่องขึ้นไป กระทำต่อคอมพิวเตอร์เครื่องเดียวหรือหลายเครือข่าย และส่งผลกระทบมหาศาล เช่น การกู้ยืม โอนเงิน ฯลฯ เหตุการณ์ดังกล่าวได้เพิ่มขึ้นหลังจากธนาคารบนมือถือและธนาคารทางอินเทอร์เน็ตเริ่มได้รับความนิยม และอาชญากรรมไซเบอร์ที่ใช้คอมพิวเตอร์บนเครือข่ายอินเตอร์เน็ตเป็นเครื่องมือในการกระทำความผิด การหลอกให้ลงทุน (Hybrid Scam) โดยอ้างว่าเป็นการลงทุนที่จะได้ผลตอบแทนสูง และท้ายที่สุดผู้อาชญากรรมไซเบอร์ก็จะฉ้อโกงเงินหนีไป ในรูปแบบสุดท้ายที่คนไทยมักจะถูกหลอกลวงมากที่สุดคือ การหลอก ลวงด้วยการโทรศัพท์ โดยแก๊งคอลเซ็นเตอร์ (Vishing Phishing) ที่สร้างสถานการณ์ที่น่ากลัวให้กับผู้เสียหายและจะอ้างว่าเป็นเจ้าหน้าที่รัฐ ถ้าผู้เสียหายขาดสติตกใจ

จากสถานการณ์ที่กล่าวมาข้างต้น สะท้อนให้เห็นถึงภัยคุกคามในโลกไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล แม้ว่าจะมีกฎหมายหรือการป้องกันจากภาครัฐแล้วก็ตาม ผู้เขียนจึงมุ่งนำเสนอสาระที่มุ่งให้รู้จักวิธีการหรือมาตรการรับมือความปลอดภัยในโลกไซเบอร์ที่สามารถป้องกันภัยคุมคามในโลกไซเบอร์ได้หากข้อมูลมีการรั่วไหล

ระดับของภัยคุกคามทางไซเบอร์ในยุคดิจิทัล

จากการศึกษาเอกสารที่เกี่ยวข้องเกี่ยวกับระดับความรุนแรงของเหตุการณ์ภัยคุกคามทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งนำไปสู่การรักษาความปลอดภัยในโลกไซเบอร์ ทั้งนี้ Pansuwan and Chitsawang (2023) แบ่งออกเป็น 3 ระดับ ได้แก่

ระดับที่ 1 ระดับไม่ร้ายแรง คือภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพ

ระดับที่ 2 ระดับร้ายแรง คือ ภัยคุกคามทางไซเบอร์ที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ ถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

ระดับที่ 3 ระดับวิกฤต ประกอบด้วย

(ก) ภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานที่สำคัญอื่นๆ อาจทำให้บุคคลจำนวนมากเสียชีวิต หรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) ภัยคุกคามทางไซเบอร์ที่กระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือสงคราม จึงจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย

จากที่กล่าวมาข้างต้นแสดงให้เห็นว่าวิถีเทคโนโลยีดิจิทัลนั้นส่งผลกระทบต่อโครงสร้างพื้นฐานของการจัดการสิ่งอำนวยความสะดวกในชีวิตประจำวัน ธุรกรรมอิเล็กทรอนิกส์ รวมทั้งการติดต่อสื่อสารต่าง ๆ ดังนั้น

ระดับของภัยคุกคามทางไซเบอร์จึงพิจารณาถึงผลกระทบที่ครอบคลุมแพร่กระจายไปมากน้อยเพียงไร ซึ่งถ้าทุกคนมีสำนึกรับผิดชอบการแพร่กระจายอาจไม่ส่งผลกระทบในระดับวิกฤติ

ประเภทของภัยคุกคามในโลกไซเบอร์

จากการศึกษาในงานวิจัยที่เกี่ยวข้องเกี่ยวกับภัยคุกคามในโลกไซเบอร์ที่สำคัญในปัจจุบันสามารถแบ่งออกเป็นหลายรูปแบบ แต่ถูกพบเจอมากที่สุด Na Pibul (2023) มีตัวอย่างดังต่อไปนี้

1. Malware เป็นคำที่มาจากคำว่า Malicious และ Software หมายถึง โปรแกรมที่ประสงค์ร้ายซึ่งถูกสร้างขึ้นเพื่อนำไปใช้ในการโจรกรรมข้อมูล ทำให้เสียหาย ทำลายคอมพิวเตอร์และระบบคอมพิวเตอร์ ตัวอย่าง Malware ที่รู้จักกันทั่วไป เช่น Viruses, Worms, Ransomware, Adware, Spyware

2. Phishing หมายถึง รูปแบบการโจมตีเหยื่อผ่านทางอีเมล ข้อความ เว็บไซต์ หรือสื่อสังคมออนไลน์ต่าง ๆ โดยใช้วิธีการหลอกให้ผู้ใช้งานหลงเชื่อและส่งมอบข้อมูลส่วนตัวให้ เช่น เลขประจำตัวประชาชน หมายเลขบัตรเครดิต หรือข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวไปใช้ซึ่งจะก่อให้เกิดความเสียหายต่อเจ้าของข้อมูล

3. DDoS (Distributed Denial of Service) Attack หมายถึง รูปแบบการโจมตี โดยการส่งชุดคำสั่งเป็นจำนวนมากไปรบกวนการทำงานโดยปกติของระบบการให้บริการ ระบบเครือข่าย หรือเซิร์ฟเวอร์ ส่งผลให้เกิดการชะลอหรือขัดขวางการทำงานจนเพื่อไม่สามารถใช้งานได้

4. Spam หมายถึง รูปแบบการส่งข้อมูล, ข้อความที่ไม่พึงประสงค์ให้กับผู้รับผ่านช่องทางต่างๆ เช่น อีเมล ข้อความ เว็บไซต์ หรือสื่อสังคมออนไลน์ต่างๆ โดยเป็นการส่งจำนวนมาก ซึ่งโดยส่วนมากจะทำไปเพื่อวัตถุประสงค์ในการโฆษณาเชิงพาณิชย์

ประเภทของภัยคุกคามในโลกไซเบอร์ดังกล่าวข้างต้นนั้นผู้โจมตีมักเน้นวิธีการที่ให้ข้อมูลเสียหายหรือถูกทำลาย ทำให้เกิดผลกระทบต่อหน่วยงานหรืองานส่วนบุคคลไม่สามารถทำงานได้ ดังนั้นสิ่งสำคัญที่สุดคือการรู้เท่าทันภัยคุกคามในโลกไซเบอร์ที่ต้องปลูกฝังตั้งแต่เด็กและเยาวชน

ภัยคุกคามในโลกไซเบอร์ที่ส่งผลกับผู้เรียนยุคดิจิทัล

ภัยคุกคามในโลกไซเบอร์ที่ส่งผลกับผู้เรียนยุคดิจิทัลคือ Diteeyon (2024) การสวมรอยหรือการปลอมแปลงทางดิจิทัล (Digital Impersonation) เป็นภัยทางไซเบอร์ที่เกิดขึ้นเป็นจำนวนมากโดยหมายถึงการบุคคลอื่นได้ปลอมตัวตนลงบัญชีช่องทางสื่อสารทางสังคมเพื่อให้เป็นเสมือนเป็นบุคคลนั้นจริง ๆ โดยส่วนมากจะเป็นปลอมบัญชีของบุคคลที่มีชื่อเสียงหรือมีฐานะทางสังคมที่ดีเพื่อต้องการให้ผู้อื่นเกิดความเชื่อถืออันจะนำไปสู่การทำกิจกรรมต่าง ๆ ได้ต่อไป เช่น การหลอกเอาข้อมูล ส่วนตัว การโอนเงิน หรือแม้แต่การล่อลวงให้ไปพบเจอเพื่อทำร้ายหรือล่วงละเมิดต่าง ๆ เป็นต้น จุดเด่นสำคัญของการปลอมแปลงทางดิจิทัล คือ ผู้ที่ทำการสวมรอยหรือปลอมแปลงบุคคลนั้นจะทำการโจรกรรมข้อมูลแทบทุกอย่างของคนที่ถูกปลอมบัญชีมาใช้ เช่น รูปภาพ สถานที่หรือแม้แต่กิจกรรมที่ทำในแต่ละวันเพื่อเป็นการทำให้ผู้อื่นเกิดความเชื่อใจให้ได้มากที่สุด แต่สำหรับในการเรียนการสอน การปลอมแปลงทางดิจิทัลที่เป็นปัญหาในกลุ่มผู้เรียนนั้นจะแบ่งออกได้เป็น 3 ประเภทดังนี้

1. การปลอมแปลงบัญชีส่วนตัว (Personal Account Impersonation) เป็นการปลอมแปลงของบัญชีของบุคคลที่มีชื่อเสียง โดยลอกเลียนแบบข้อมูลของบุคคลนั้นเกือบทุกอย่างลงในบัญชีใหม่ที่ทำขึ้นมาเพื่อเป้าหมายในการหลอกลวงเพื่อหวังผลประโยชน์ทางการเงินหรือเพิ่มยอดการติดตาม (Followers) สำหรับการปลอมแปลงบุคคลทางดิจิทัลที่เกี่ยวข้องกับผู้เรียน ส่วนมากจะเป็นการปลอมแปลงบัญชีเป็นผู้อื่น

เพื่อการกลั่นแกล้งทางไซเบอร์ไม่ว่าจะเป็นการปล่อยข้อมูลเท็จเพื่อสร้างความสับสนหรือการนินทาว่าร้ายกับผู้เรียนท่านอื่น เป็นต้น

2. การยึดครองบัญชีสื่อสารสังคม (Social Media Account Hijacking) เป็นการยึดครองการเข้าสู่ระบบของบัญชีช่องทางการสื่อสารสังคมของบุคคลอื่นโดยไม่ได้ยินยอม ส่วนมากจะเป็นบัญชีทาง Facebook, YouTube หรือ Instagram โดยเจ้าของบัญชีจะไม่สามารถเข้าสู่ระบบบัญชีของตนเองได้อีกต่อไป สำหรับผู้เรียนนั้น การยึดครองบัญชีสื่อสารทางสังคมนี้จะมีเป้าหมายเพื่อการกลั่นแกล้งทางไซเบอร์และการทำกิจกรรมที่เกี่ยวข้องกับคนจำนวนมาก เช่น การเผยแพร่ข่าวสารเป็นเท็จ การขโมยข้อมูลส่วนตัวหรือการ สร้างพฤติกรรมที่ไม่เหมาะสมของเจ้าของบัญชีเดิม เป็นต้น

3. ปลอมบัญชีบุคคล (Fake Accounts or Bots) เป็นการสร้างบัญชีปลอมขึ้นมาที่ทำงานโดยระบบหรือหุ่นยนต์ (Bot) เพื่อประชาสัมพันธ์ข่าวสาร การส่งข้อความอัตโนมัติ หรือการเข้าถึงกลุ่มต่าง ๆ โดยบัญชีช่องทางสื่อสารสังคมเหล่านี้จะที่ไม่มีบุคคลจริงในการกระทำกิจกรรมดังกล่าว แต่เป็นระบบคอมพิวเตอร์ที่ทำกิจกรรมเหล่านั้นเท่านั้น สำหรับผู้เรียนนั้น ภัยอันตรายประเภทนี้เกิดขึ้นเพื่อหวังผลหลอกลวงทางการเงินและการเจาะเอาข้อมูลส่วนตัวเป็นสำคัญ

จากที่กล่าวมาข้างต้นแสดงให้เห็นว่าภัยคุกคามในโลกไซเบอร์ที่ส่งผลกับผู้เรียนยุคดิจิทัลนั้น จะมุ่งเน้นข้อมูลส่วนบุคคลที่เด็กและเยาวชนต้องตระหนักในการรักษาข้อมูลส่วนตัว และมีสติ สำนึกความรับผิดชอบในการสื่อสารผ่านสื่อสังคม

เทคโนโลยีอัจฉริยะบิดดีเฟนเดอร์ สคามิโอ กับภัยคุกคามในโลกไซเบอร์

ปัญญาประดิษฐ์ (AI) ซึ่งเป็นเทคโนโลยีอัจฉริยะได้มีบทบาทสำคัญทั้งในการป้องกันภัยคุกคามในโลกไซเบอร์ โดยมีผลกระทบทางกับผู้เรียนในยุคดิจิทัลอย่างมีนัยสำคัญ ปัญญาประดิษฐ์ถูกนำมาใช้หลากหลายด้าน เช่น การช่วยเหลือในการค้นหาหรือสรุปข้อมูล Verma and Gupt (2020) การเพิ่มประสิทธิภาพด้านความปลอดภัยทางไซเบอร์โดยการตรวจจับและลดภัยคุกคามได้อย่างรวดเร็วและแม่นยำกว่าวิธีการแบบดั้งเดิมเช่น การใช้เทคนิคการเรียนรู้ของเครื่อง (Machine Learning) สำหรับการตรวจจับการฉ้อโกงและป้องกันการโจมตี Hoanca and Mock (2020) อย่างไรก็ตามอาชญากรไซเบอร์สามารถใช้ปัญญาประดิษฐ์ในการขยายขนาดการโจมตีทางไซเบอร์ทาให้เกิดช่องทางใหม่สำหรับการก่ออาชญากรรมไซเบอร์ ปัญญาประดิษฐ์กำลังเติบโตอย่างรวดเร็วซึ่งเน้นย้ำถึงความสำคัญในการลดความสูญเสียทางการเงินจากการโจมตีในโลกไซเบอร์ ทั้งนี้ บิดดีเฟนเดอร์ สคามิโอ (Bitdefender Scamio) เป็นโปรแกรมที่ถูกพัฒนาโดย SOFTWIN ซึ่งเป็นบริษัทที่ก่อตั้งในปี 1990 ซึ่งเป็นซอฟต์แวร์ในการรักษาความปลอดภัยในโลกไซเบอร์ ซึ่งปัจจุบัน บิดดีเฟนเดอร์ สคามิโอ เปิดตัวเครื่องตรวจจับการหลอกลวงที่ขับเคลื่อนด้วย AI ซึ่ง จากการศึกษาถึงคุณสมบัติของบิดดีเฟนเดอร์ สคามิโอ พบว่า เป็นซอฟต์แวร์ที่ถูกพัฒนามาอย่างต่อเนื่องและครอบคลุมปัญหาความปลอดภัยในโลกไซเบอร์ทั้งส่วนบุคคลและองค์กร ซึ่ง Mailmaster (2024) ได้กล่าวถึงคุณสมบัติของบิดดีเฟนเดอร์ สคามิโอ ไว้ดังนี้

1. สามารถตรวจจับมัลแวร์ตัวอย่างได้ทุกประเภท ด้วยระบบสแกนไวรัสบนคลาวด์ช่วยให้คอมพิวเตอร์ทำงานได้เร็วขึ้น ชาญฉลาด และยังใช้ระบบ AI เข้ามาช่วยตรวจจับภัยคุกคาม สามารถตรวจจับเว็บปลอมและเว็บที่มีความเสี่ยงมากกว่าเครื่องมือป้องกันในตัวจาก Chrome, Firefox หรือ Edge และการป้องกันฟิชชิ่งจากโปรแกรมป้องกันไวรัสอื่นๆ

2. ป้องกันแบบเรียลไทม์ (Real-time protection) ช่วยป้องกันไม่ให้ไวรัส มัลแวร์ และภัยคุกคามทางไซเบอร์อื่นๆ เข้าสู่อุปกรณ์ของคุณ

3. การสแกนแบบกำหนดเอง (Custom scan) ช่วยให้คุณสแกนอุปกรณ์ของคุณเพื่อหาภัยคุกคามที่เฉพาะเจาะจง

4. การกรองอีเมล (Email filtering) ช่วยป้องกันไม่ให้อีเมลที่เป็นอันตรายเข้าสู่กล่องจดหมาย

5. การปกป้องเว็บ (Web protection) ช่วยป้องกันไม่ให้คุณเข้าสู่เว็บไซต์ที่เป็นอันตราย

6. การป้องกัน Wi-Fi (Wi-Fi protection) ช่วยปกป้องการเชื่อมต่อ Wi-Fi จากภัยคุกคาม

7. การป้องกันเครือข่าย (Network protection) ช่วยป้องกันอุปกรณ์ของคุณจากภัยคุกคามที่แพร่กระจายผ่านเครือข่าย

8. ฟีเจอร์ในการควบคุมโดยผู้ปกครอง (Parental Control) ด้วยเทคโนโลยีขั้นสูง เพื่อให้บุตรหลานของคุณปลอดภัยจากภัยคุกคามทางออนไลน์

9. VPN คุณภาพสูง: บริการ VPN ของ Bitdefender มีความเร็วและประสิทธิภาพเทียบเท่ากับ VPN แบบสแตนด์อโลนและมาพร้อมกับความสามารถในการปรับแต่งสูง และความสามารถอื่นๆ อีกมากมาย

จากที่กล่าวมาข้างต้นบิดดีเฟนเดอร์ สคามิโอ มีคุณสมบัติที่ครอบคลุมความปลอดภัยในโลกไซเบอร์ทั้งในระดับบุคคลถึงระดับหน่วยงาน องค์กร ดังนั้นภัยคุกคามที่หลากหลายซึ่งถูกพัฒนาขึ้นมาด้วยวัตถุประสงค์ทั้งในด้านข้อมูลของผู้ใช้ หรือก่อให้เกิดอุปสรรคในการติดต่อสื่อสารบิดดีเฟนเดอร์ สคามิโอจึงเป็นทางเลือกในการใช้งานเพื่อรักษาความปลอดภัยของข้อมูลบนเครือข่ายอินเทอร์เน็ต

การใช้งานบิดดีเฟนเดอร์ สคามิโอ

การใช้บิดดีเฟนเดอร์ สคามิโอ (Bitdefender Scamio) เกี่ยวข้องกับการใช้ประโยชน์จากปัญญาประดิษฐ์ขั้นสูง (AI) เพื่อตรวจจับและวิเคราะห์กลโกงออนไลน์ที่อาจเกิดขึ้น ผู้ใช้สามารถส่งเนื้อหาที่น่าสงสัย เช่น อีเมล ข้อความ หรือลิงก์ ไปยังโปรแกรม ซึ่งจะวิเคราะห์และให้ผลลัพธ์ภายในไม่กี่วินาที สิ่งนี้จะช่วยให้ผู้ใช้ระบุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เช่น ความพยายามฟิชชิ่งหรือกิจกรรมฉ้อโกง และรับประกันประสบการณ์ออนไลน์ที่ปลอดภัยยิ่งขึ้น บิดดีเฟนเดอร์ สคามิโอ เป็นเครื่องมืออันทรงคุณค่าในการเพิ่มความปลอดภัยทางไซเบอร์ โดยเฉพาะอย่างยิ่งในบริบททางการศึกษาที่ผู้เรียนจะได้รับประโยชน์ในการรับรู้ที่เพิ่มขึ้นและการป้องกันความเสี่ยงทางดิจิทัล ทั้งนี้มีลักษณะการใช้งานดังนี้ SafetyDetectives (2025)

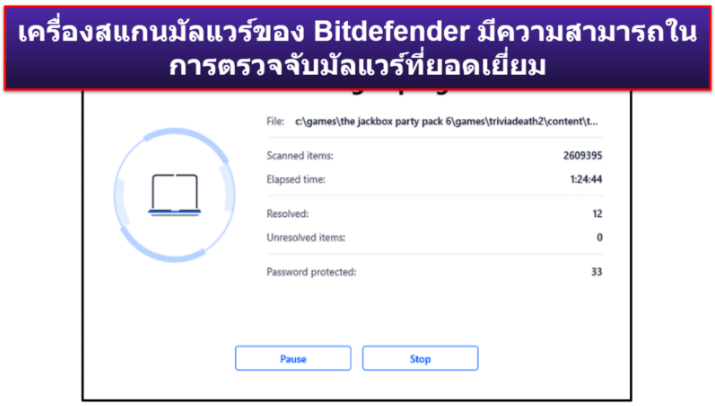
1. ฟีเจอร์ด้านความปลอดภัยของบิดดีเฟนเดอร์ สคามิโอ สแกนไวรัส ที่ทำงานได้ละเอียดและมีขนาดเล็ก โดยใช้ไดเรกทอรีมัลแวร์ขนาดใหญ่และใช้การเรียนรู้ของเครื่องเพื่อตรวจจับมัลแวร์ทั้งที่เป็นที่รู้จักและมัลแวร์ใหม่ และเนื่องจากการสแกนมัลแวร์ส่วนใหญ่เกิดขึ้นในระบบคลาวด์ โปรแกรมแอนตี้ไวรัสของ Bitdefender จึงใช้ CPU และพื้นที่ดิสก์เพียงเล็กน้อยในระหว่างการสแกน Bitdefender มีการสแกน 4 ประเภท:

1.1 Quick Scan การสแกนที่ใช้ทรัพยากรน้อยที่สแกนไฟล์ระบบหลักและไฟล์ชั่วคราวซึ่งมักจะเก็บไวรัสไว้

1.2 System Scan การวิเคราะห์เชิงลึกและการสแกนระบบทั้งหมดเพื่อหามัลแวร์และช่องโหว่

1.3 Custom Scan การสแกนในตำแหน่งระบบใด ๆ ที่อาจมีภัยคุกคาม

1.4 Vulnerability Scan การสแกนหาความเสี่ยงด้านความเป็นส่วนตัวในการตั้งค่าแอปพลิเคชัน ตลอดจนการอัปเดตซอฟต์แวร์ที่สำคัญ ดังภาพที่ 1



ภาพที่ 1 แสดงการใช้งานบิดดีเฟนเดอร์ สคามิโอในการสแกนมัลแวร์
ที่มา: https://th.safetydetectives.com/best-antivirus/bitdefender/

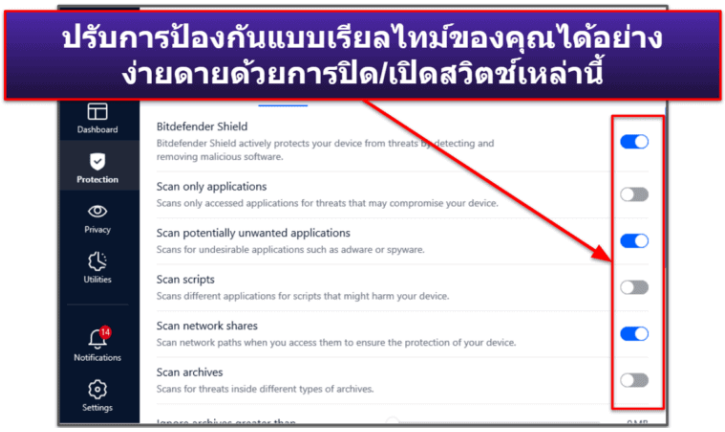
2. การป้องกันแบบเรียลไทม์ การป้องกันแบบเรียลไทม์ของ Bitdefender (Bitdefender Shield) จะสแกนทุกไฟล์และไฟล์แนบอีเมลทันทีที่เข้าถึง การตั้งค่าเริ่มต้นของ Bitdefender Shield ประกอบด้วยการสแกนต่อไปนี้:

2.1 แอปพลิเคชันที่อาจไม่ต้องการ ซอฟต์แวร์ที่ซ่อนอยู่ในแอปพลิเคชันอื่น ๆ (โดยปกติจะมีฟรีแวร์)

2.2 การแบ่งปันเครือข่าย ปัญหาในเครือข่ายระยะไกลบนอุปกรณ์ส่วนบุคคล

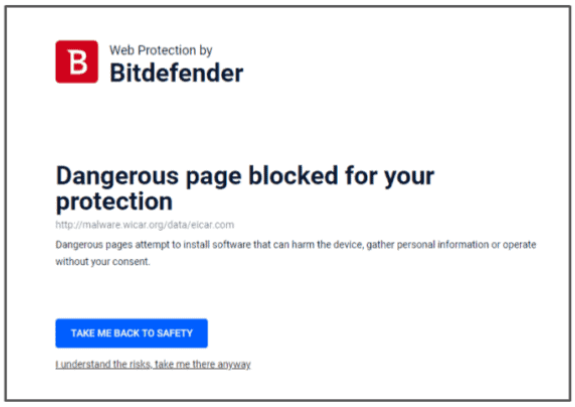
2.3 บูตเซกเตอร์ ปัญหาที่อาจทำให้ลำดับการบูตอุปกรณ์ของผู้ใช้เปลี่ยนไป เฉพาะไฟล์ใหม่และไฟล์ที่แก้ไข ภัยคุกคามที่อาจซ่อนอยู่ในไฟล์ใหม่และไฟล์ที่แก้ไข

2.4 Keyloggers (คีย์ล็อกเกอร์) มัลแวร์ที่ตรวจจับการกดแป้นพิมพ์แม้ว่าการป้องกันเริ่มต้นของ Bitdefender Shield จะดีพอสำหรับผู้ใช้ส่วนใหญ่ แต่ผู้ใช้ขั้นสูงก็สามารถปรับแต่งการตั้งค่าแบบเรียลไทม์ เพื่อรวมการป้องกันในแอปพลิเคชัน สคริปต์และไฟล์เก็บถาวรได้ ผู้ใช้ขั้นสูงยังสามารถเลือกที่จะยกเว้นตัวเลือกใด ๆ ที่กล่าวถึงข้างต้นได้



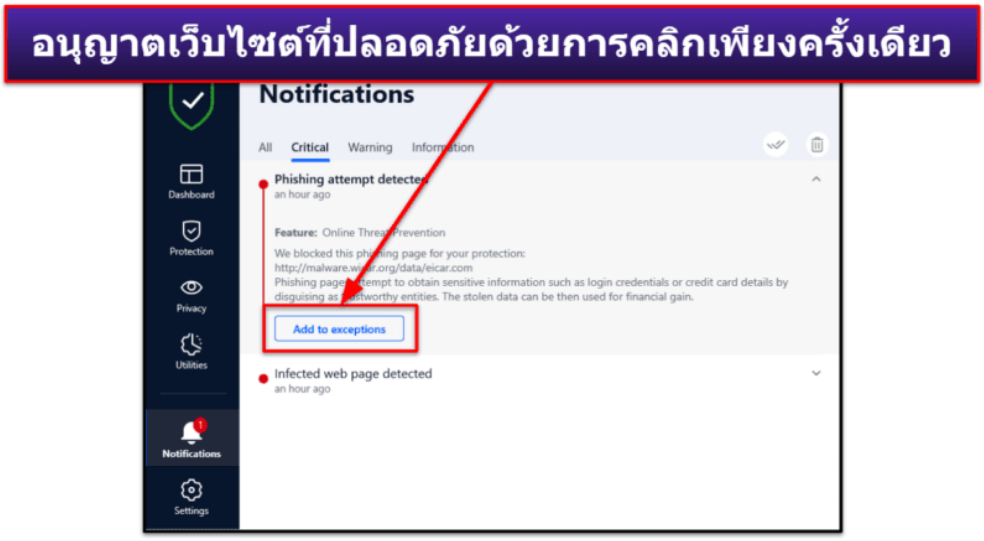
ภาพที่ 2 แสดงการใช้งานบิดดีเฟนเดอร์ สคามิโอในในการป้องกันแบบเรียลไทม์
ที่มา: https://th.safetydetectives.com/best-antivirus/bitdefender/

3. การป้องกันฟิชชิ่ง/การป้องกันเว็บ เมื่อใดก็ตามที่เยี่ยมชมเว็บไซต์การป้องกันฟิชชิ่งของ Bitdefender จะเปรียบเทียบข้อมูลกับฐานข้อมูลที่มีการอัปเดตเป็นประจำซึ่งมีรายการเว็บไซต์ที่เป็นอันตรายและอยู่ในบัญชีดำหลายล้านรายการ หากข้อมูลนั้นอยู่ในรายการ Bitdefender จะบล็อกการเข้าถึงเว็บไซต์ ดังภาพที่ 3



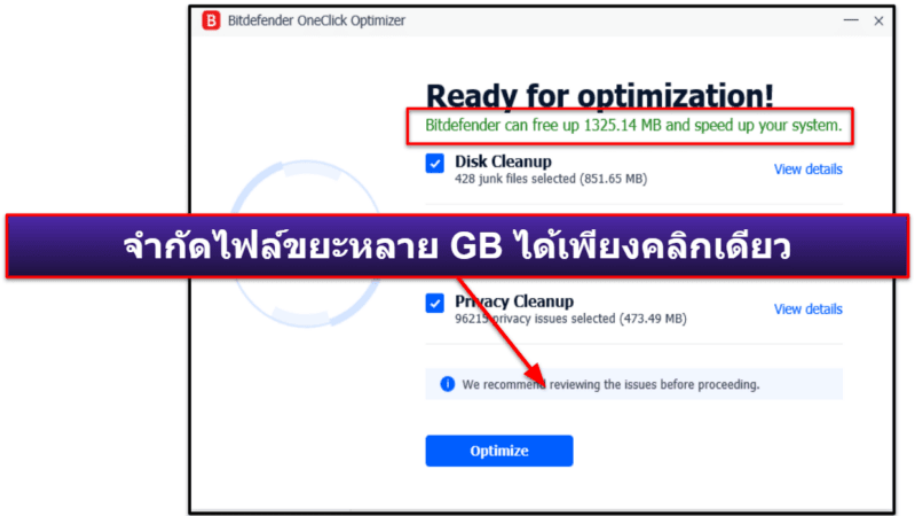
ภาพที่ 3 แสดงการใช้งานบิดดีเฟนเดอร์ สคามิโอในในการป้องกันฟิชชิ่ง/การป้องกันเว็บ
ที่มา: https://th.safetydetectives.com/best-antivirus/bitdefender/

Bitdefender ยังมีหน้าจอการแจ้งเตือนที่สะดวก ที่สามารถดูได้ว่าเว็บไซต์ใดที่ถูกบล็อกและทำไม ทำให้ง่ายต่อการป้องกันความผิดพลาดในรายการยกเว้นของ Bitdefender อย่างถาวร โดยผู้ใช้สามารถอนุญาตเว็บไซต์พิเศษได้ในคลิกเดียว ในขณะที่โปรแกรมป้องกันไวรัสอื่น ๆ เช่น Norton ต้องการให้เราเจาะลึกการตั้งค่าและโปรโตคอลขั้นสูงเพื่อเพิ่มไซต์ที่ปลอดภัย อย่างไรก็ตามโปรดทราบว่าเราควรอนุญาตเฉพาะเว็บไซต์ที่มั่นใจอย่างยิ่งว่าเว็บไซต์เหล่านั้นถูกต้องตามกฎหมายและไม่มีมัลแวร์ ดังภาพที่ 4



ภาพที่ 4 แสดงการแจ้งเตือนของการใช้งานบิดดีเฟนเดอร์ สคามิโอ
ที่มา: https://th.safetydetectives.com/best-antivirus/bitdefender/

4. การเพิ่มประสิทธิภาพระบบในเครื่องคอมพิวเตอร์ โดยใช้เครื่องมือ OneClick Optimizer ของ Bitdefender เป็นเครื่องมือที่ให้บริการแบบพื้นฐาน ซึ่งมีประโยชน์สำหรับการเพิ่มพื้นที่ว่างในดิสก์บนคอมพิวเตอร์ โดยจะสแกนระบบและลบไฟล์ที่ไม่จำเป็นออกจากอุปกรณ์ แต่มันให้บริการได้ธรรมดามากเมื่อเทียบกับคู่แข่งอย่าง Avira (ซึ่งมีเครื่องมือเพิ่มประสิทธิภาพการบูต เกมบูสเตอร์ เครื่องมือจัดการอัปเดตไดรเวอร์และการใช้แบตเตอรี่) Bitdefender จะลบไฟล์ขยะต่าง ๆ ซึ่งรวมถึง ไฟล์ระบบชั่วคราว ไฟล์ขยะของ Windows ไฟล์ถังขยะ รายการรีจิสทรีที่ใช้ไม่ได้แล้ว และประวัติการใช้งาน ดังภาพที่ 5



ภาพที่ 5 แสดงการเพิ่มประสิทธิภาพระบบในเครื่องคอมพิวเตอร์ โดยใช้เครื่องมือ OneClick Optimizer
ที่มา: https://th.safetydetectives.com/best-antivirus/bitdefender/

จากที่กล่าวมาข้างต้นแสดงให้เห็นถึงศักยภาพการใช้งานของซอฟต์แวร์บิดดีเฟนเดอร์ สคามิโอ (Bitdefender Scamio) ที่ผสานกับการใช้ประโยชน์จากปัญญาประดิษฐ์ขั้นสูง (AI) เพื่อตรวจจับและวิเคราะห์กลโกงออนไลน์ในรูปแบบการวิเคราะห์ตรวจจับแบบ 360 องศา ที่ผู้ใช้เทคโนโลยีดิจิทัลควรปกป้องข้อมูลและระบบ และสร้างสภาพแวดล้อมการเรียนรู้ที่ปลอดภัยและทักษะสำหรับผู้เรียนยุคดิจิทัล

บทบาทของผู้เรียนยุคดิจิทัลในการใช้บิดดีเฟนเดอร์ สคามิโอ กับความปลอดภัยในโลกไซเบอร์

ผู้เรียนยุคดิจิทัล คือ บุคคลที่ภายใต้สภาพแวดล้อมการเรียนรู้ออนไลน์ ทรัพยากรดิจิทัล ซึ่งบุคคลดังกล่าวต้องมีความพร้อมที่จะเรียนรู้และปรับตัวตลอดเวลา การเข้าถึงแหล่งข้อมูลออนไลน์ และทรัพยากรดิจิทัลอื่น ๆ ช่วยให้ผู้เรียนสามารถพัฒนาตนเองอย่างต่อเนื่อง และผู้เรียนต้องมีทักษะในการค้นหา วิเคราะห์และประเมินข้อมูล เป็นสิ่งที่ขาดไม่ได้ในกระบวนการเรียนรู้เพื่อความปลอดภัยในโลกไซเบอร์ อย่างไรก็ตามการใช้งานเทคโนโลยีเหล่านี้ยังแฝงไปด้วยความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ Office of the Basic Education Commission (2023) บทบาทสำคัญของผู้เรียนในการใช้บิดดีเฟนเดอร์ สคามิโอ เพื่อเสริมสร้างการเรียนรู้ความปลอดภัยในโลกไซเบอร์ตามหลักสูตร สาระเทคโนโลยี (วิทยาการคำนวณ) มีดังนี้

1. ผู้เรียนได้เรียนรู้จากข่าวหรือสถานการณ์ปัญหาที่หน่วยงานหรือบุคคลถูกการปลอมแปลงข้อมูลและเข้าถึงข้อมูลส่วนบุคคล หลังจากนั้นแสดงให้เห็นถึงการใช้งานตัวอย่างซอฟต์แวร์บิดดีเฟนเดอร์ สคามิโอ หลังจากนั้นร่วมกันอภิปรายเพื่อฝึกการวิเคราะห์อย่างมีวิจารณญาณให้เกิดการตระหนักรู้และการเรียนรู้

เกี่ยวกับความปลอดภัยในโลกไซเบอร์ ผู้เรียนควรมีความรู้พื้นฐานเกี่ยวกับภัยคุกคามในโลกไซเบอร์และวิธีการป้องกัน เช่น การสร้างรหัสผ่านที่ปลอดภัย การหลีกเลี่ยงลิงก์ที่ไม่น่าเชื่อถือ และการใช้งานซอฟต์แวร์ป้องกันไวรัส

2. ผู้เรียนเขียนแผนที่ความคิดจากสถานการณ์ที่เป็นข่าวผ่านสื่อสังคมในประเด็นการพัฒนาทักษะการใช้เทคโนโลยีอย่างรับผิดชอบโดยให้ผู้เรียนระบุประเด็นการใช้งานเทคโนโลยีอย่างปลอดภัยและมีความรับผิดชอบ เช่น วิธีการปฏิบัติตามแนวทางการใช้งานสื่อสังคม (Social Media) อย่างปลอดภัย วิธีการปกป้องข้อมูลส่วนบุคคล และวิธีการไม่เผยแพร่ข้อมูลที่อาจเป็นอันตรายต่อผู้อื่น

3. ผู้เรียนแสดงการเป็นผู้นำในการสร้างวัฒนธรรมความปลอดภัยในชุมชนการเรียนรู้ในกลุ่มโดยผู้เรียนวิเคราะห์ผลการตรวจสอบผลการสแกนไวรัส มัลแวร์ จากการใช้งานตัวอย่างซอฟต์แวร์บิดดีเฟนเดอร์ สคามิโอ โดยอธิบายถึงบทบาทในการสร้างวัฒนธรรมที่ส่งเสริมความปลอดภัยในโลกไซเบอร์ โดยการแบ่งปันความรู้กับเพื่อนร่วมชั้น การรายงานเหตุการณ์ที่น่าสงสัย และการส่งเสริมการใช้งานเทคโนโลยีอย่างปลอดภัยในกลุ่มเพื่อน

จากข้อความดังกล่าวข้างต้นบทบาทของผู้เรียนยุคดิจิทัลในการใช้บิดดีเฟนเดอร์ สคามิโอต่อการเสริมสร้างความปลอดภัยในโลกไซเบอร์ที่มีรอบด้าน นั้นผู้เรียนต้องเกิดกระบวนการเรียนรู้โดยเกิดทักษะกระบวนการคิด และกิจกรรมการเรียนรู้เชิงรุก (Active Learning) ซึ่งผู้สอนต้องใช้สื่อประสบการณ์แห่งการเรียนรู้ของเอดการ์เดลที่มุ่งเน้นการถ่ายทอดประสบการณ์จากนามธรรมไปสู่รูปธรรม

บทบาทของผู้สอนยุคดิจิทัลที่มีต่อการเสริมสร้างความปลอดภัยในโลกไซเบอร์

จากการศึกษาเอกสารที่เกี่ยวข้องพบว่าผู้สอนต้องปรับเปลี่ยนกระบวนการจัดการเรียนการสอน รวมทั้งต้องพัฒนาตนเอง โดยบทบาทของของผู้สอนยุคดิจิทัลนั้นต้องมีการสร้างสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยแก่ผู้เรียนเพื่อให้ผู้เรียนตระหนักรู้จักการรักษาความปลอดภัยในโลกไซเบอร์ที่ ซึ่ง Diteeyon (2024) และ Fasulo (2021) อธิบายไว้ดังนี้

การสร้างสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยในการจัดการเรียนการสอนของครูยุคดิจิทัล จำเป็นต้องพิจารณาถึงคุณสมบัติของความปลอดภัยทางไซเบอร์ (CIA Trait) ที่ประกอบไปด้วยหลักพื้นฐาน 3 ประการที่สถานศึกษา ผู้สอนและนักการศึกษาควรตระหนักและทำให้เกิดขึ้นเพื่อให้สภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยให้แก่ผู้เรียนได้ ทั้งนี้การออกแบบสภาพแวดล้อมการเรียนการสอนทางไซเบอร์ที่ปลอดภัย ประกอบด้วย

1. สภาพแวดล้อมการเรียนรู้ที่ก่อให้เกิดความมั่นใจ (Confidentiality Learning Environment) คือ ผู้สอนต้องอธิบายให้ผู้เรียนเกิดความมั่นใจและตระหนักโดยแสดงถึงขั้นตอนในการเข้าชั้นเรียนด้วยสภาพแวดล้อมทางไซเบอร์ปลอดภัยซึ่งต้องประกอบไปด้วยความรู้สึกมั่นใจของผู้ใช้งานในการเข้าถึง เผยแพร่และเก็บรักษาข้อมูลภายในสภาพแวดล้อมทางไซเบอร์

2. สภาพแวดล้อมการเรียนรู้เพื่อสร้างความซื่อสัตย์ (Integrity Learning Environment) สภาพแวดล้อมทางไซเบอร์ที่ปลอดภัยจำเป็นต้องประกอบไปด้วยข้อมูลที่ถูกต้องเพื่อทำให้ผู้เรียนนั้นสามารถเกิดเรียนรู้ได้อย่างมีประสิทธิภาพ รวมไปถึงไม่ตกอยู่ในสภาวะ ไม่ตกอยู่ในภาวะตื่นกลัวหรือมีโอกาสในการตกเป็นเหยื่อจากอาชญากรรมทางไซเบอร์ได้ซึ่งสถานศึกษาควรเลือกใช้เครื่องมือหรือระบบที่มีการตรวจสอบข้อมูลที่เชื่อมต่อกับฐานข้อมูลภายนอกได้อย่างรวดเร็ว ระบบคัดกรองข้อมูล หรือระบบการรายงานข้อมูลกับหน่วยงานภายนอก นอกจากนั้น สถานศึกษาควรมีหน่วยที่ประกอบไปด้วยบุคคลที่มีหน้าที่ตรวจสอบการเผยแพร่ข้อมูลทางไซเบอร์ รวมไปถึงบุคคลที่มีหน้าที่เกี่ยวข้องกับกฎหมาย เพื่อเป็นการช่วยเหลือให้เกิดการเผยแพร่ข้อมูลที่ถูกต้องในสภาพแวดล้อมนั้นต่อไป

3. สภาพแวดล้อมการเรียนรู้ที่แสดงถึงความพร้อม (Availability Learning Environment) คือผู้สอนต้องกำหนดสภาพแวดล้อมทางไซเบอร์ที่ปลอดภัย โดยอาจมีมาตรการและให้ผู้เรียนอ่านข้อเตือนสติถึงความพร้อมในการเข้าถึงหรือเข้าใช้ข้อมูลออนไลน์ ทั้งนี้จะต้องประกอบไปด้วยข้อมูลที่หลากหลายและเพียงพอต่อความต้องการของผู้เรียน รวมไปถึงความต่อเนื่องในการใช้ข้อมูลและการให้บริการข้อมูลในสภาพแวดล้อมด้วย ซึ่งสถาบันการศึกษาควรส่งเสริมความพร้อมนี้โดยเลือกใช้เครื่องมือที่มีการจัดการข้อมูลดิจิทัลที่มีความเสถียร ระบบการเชื่อมต่อที่มีประสิทธิภาพ เช่น ระบบปฏิบัติการหลังบ้านที่สามารถจัดการข้อมูลต่าง ๆ หน่วยความจำที่เพียงพอในการเก็บข้อมูล หรือระบบไซเบอร์ที่มีความเสถียรในการกระจายสัญญาณเครือข่าย เป็นต้น

จากที่กล่าวมาข้างต้นสภาพแวดล้อมการเรียนรู้ (Learning Environment) เป็นสิ่งสำคัญสำหรับครูในยุคดิจิทัลต้องปรับเปลี่ยนเพื่อให้ผู้เรียนได้เข้าถึง เข้าใจ และเรียนรู้ ซึ่งถ้าต้องการสอนในประเด็นใดก็ควรออกแบบสภาพแวดล้อมการเรียนรู้ให้เหมาะสมกับตัวชี้วัดนั้น ๆ ซึ่งถ้าต้องการสอนความปลอดภัยในโลกไซเบอร์ ผู้สอนต้องออกแบบสภาพแวดล้อมการเรียนรู้ที่ก่อให้เกิดความมั่นใจ การสร้างความซื่อสัตย์ และมีความพร้อม ทั้งนี้ผู้เรียนจะเกิดเรียนรู้จากแบบอย่างดังกล่าวและนำไปปรับใช้ในชีวิตประจำวันได้

สรุปองค์ความรู้

การนำเทคโนโลยีอัจฉริยะบิดดีเฟนเดอร์ สคามิโอ เพื่อเสริมสร้างความปลอดภัยในโลกไซเบอร์ของผู้เรียนยุคดิจิทัล เป็นเพิ่มประสิทธิภาพในการเรียนการสอนที่เน้นความปลอดภัยให้ผู้เรียนยุคดิจิทัล รู้จักใช้เทคโนโลยีปัญญาประดิษฐ์ และใช้หลักการองค์ความรู้ที่หลากหลาย ผู้สอนต้องมีการออกแบบกิจกรรมเป็นกระตุ้นความสนใจ และเป็นประโยชน์ต่อผู้เรียนในยุคดิจิทัล สอดคล้องกับการเรียนรู้ในศตวรรษที่ 21 ที่เน้นทักษะการใช้เทคโนโลยีดิจิทัลในชีวิตประจำวัน และการเรียนรู้ของผู้เรียนตามความเป็นจริง เพื่อที่จะสามารถรู้เท่าทันภัยคุกคามในโลกไซเบอร์ได้อย่างเหมาะสม นอกจากนี้ ผู้เรียนและผู้สอนในยุคดิจิทัลยังสามารถนำไปพัฒนาต่อยอดเพื่อส่งเสริมการรู้เท่าทันภัยคุกคามในโลกไซเบอร์ด้วยการพัฒนากระบนการคิดของผู้คนในระดับชุมชน สังคม และประเทศชาติอย่างมีประสิทธิภาพในอนาคต โดยผู้สอนจำเป็นต้องออกแบบการเรียนการสอนโดยให้ผู้เรียนได้เรียนรู้จากการใช้งานตัวอย่างซอฟต์แวร์บิดดีเฟนเดอร์ สคามิโอ รวมทั้งการออกแบบสภาพแวดล้อมการเรียนรู้ที่ครอบคลุมสภาพแวดล้อมรู้ที่ให้เห็นตัวอย่างที่ระบบความปลอดภัยในโลกไซเบอร์มีความมั่นใจ ให้เห็นถึงความซื่อสัตย์ และการสร้างความพร้อมของระบบออนไลน์ ดังนั้นในยุควู้ก้าที่ดิจิทัลมีความผันผวนเทคโนโลยีได้กลายเป็นส่วนหนึ่งของชีวิตประจำวัน สถานศึกษาจะต้องปรับตัวในการนำเทคโนโลยีมาใช้ซึ่งอาจมีความเสี่ยง เป็นเหตุผลที่สถานศึกษาจึงต้องให้ความสำคัญกับความปลอดภัยในโลกไซเบอร์ เทคโนโลยีมีความก้าวหน้าอย่างรวดเร็ว การให้ความสำคัญกับความปลอดภัยในโลกไซเบอร์เป็นสิ่งจำเป็น สถานศึกษาต้องพร้อมรับมือกับภัยคุกคามทางไซเบอร์ ไม่เพียงเพื่อปกป้องข้อมูลและระบบเท่านั้น แต่ยังเพื่อสร้างสภาพแวดล้อมการเรียนรู้ที่ปลอดภัยและทักษะสำหรับผู้เรียนยุคดิจิทัลในอนาคต

References

Diteeyon, W. (2024). Approaches for enhancing cyber security among learners. *Academic Journal of Thailand National Sports University, 16*, 291-302.

Electronic Transactions Development Agency. (2021). *CS101 Basics of Cyber Security*. Retrieved December 2, 2024, from https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/Articles/Cybersecurity-101.aspx

Fasulo, P. (2021). What is the CIA trait? Definition, importance, & example. Retrieved December 2, 2024, from https://securityscorecard.com/blog/what-is-the-cia-triad/

Hoanca, B., & Mock, K. J. (2020). Artificial intelligence-based cybercrime. In M. Khosrow-Pour (Ed.), *Encyclopedia of Criminal Activities and the Deep Web* (2020, pp. 36-51).

Khurunun, K., & Saengthongdee, T. (2023). Guidelines for preventing cybercrime in Thailand. *Journal of Legal Entity Management and Local Innovation, 9*(6), 180-190.

Mailmaster. (2024). *Bitdefender (Antivirus Software)*. Retrieved December 2, 2024,

Na Pibul, A. (2023). The correlations between the concept of cybersecurity and the personal data protection law. *Nitipat NIDA Law Journal, 12*, 84-107.

Novak, D. (2024). *Bitdefender Scamio – Scam Detector (REVIEW)*. Retrieved December 2, 2024, from https://www.linkedin.com/pulse/bitdefender-scamio-next-gen-ai-powered-scam-detector-chatbot-novak-mf8fc

Office of the Basic Education Commission. (2023). *Unhealthiness*. Retrieved December 2, 2024, from https://main.spmnonthaburi.go.th/wp-content/uploads/2024/04/ไซเบอร์.pdf

Pansuwan, C., & Chitsawang, S. (2023). Guidelines on corporate governance for responding to cybersecurity threats in the digital age. *Rajapark Journal, 17*(53), 103-119.

Putwattana, P. (2021). Learning management for developing learners in the digital age. *Journal of Learning Innovation and Technology, 1*(2), 1-10.

SOSECURE. (2024). *Summary of 9 major cyber attacks in Thailand*. Retrieved December 2, 2024, from https://www.sosecure.co.th/en/activity/cyber-attack

SafetyDetectives. (2025). *Bitdefender Review 2025: Is it a good antivirus?* Retrieved January 2, 2025, from https://th.safetydetectives.com/best-antivirus/bitdefender/

Thaihealth. (2024). Thaihealth collaborates with Chulalongkorn University's Faculty of Economics to delve into online threats, revealing that 36 million Thais have been scammed, resulting in nearly 50 billion baht in losses. Retrieved December 2, 2024, from https://www.thaihealth.or.th/?p=362488