การประยุกต์หลักพุทธธรรมเพื่อรับมือภัยคุกคามออนไลน์

Applying Buddhist principles to cope with online threats.

1. พระธีรพล ณฏฐิโก (บัวทอง)*, 2. พัชริน จินดาปทีป

1. PhraTerapon Nutthiko, 2. Patcharin Jindapateep

1. มหาวิทยาลัยรามคำแหง, 2. มหาวิทยาลัยเกษตรศาสตร์

1. Ramkhamhaeng University, 2. Kasetsart University

Author E-mail: benedit8263@gmail.com*

บทคัดย่อ

บทความวิชาการนี้มีวัตถุประสงค์เพื่อศึกษาวิเคราะห์การประยุกต์หลักพุทธธรรมเพื่อรับมือภัยคุกคามออนไลน์ พบว่า ภัยคุกคามทางดิจิทัลในยุคปัจจุบันมีความซับซ้อนและหลากหลายมากขึ้นตามการพัฒนาของเทคโนโลยี เพื่อหลอกลวงหรือโจมตีเป้าหมายเป็นอาชญากรรมในยุคใหม่ที่เรียกว่า“อาชญากรรมไซเบอร์” หลักธรรมในพระพุทธศาสนาที่สอนให้คนรู้จักใช้ปัญญาพิจารณา เช่น หลัก “เกสปุตตสูตร” หรือ “กาลามสูตร” ไม่ให้เชื่อสิ่งใดโดยง่าย หลักการนี้สามารถนำมาประยุกต์ใช้กับภัยดิจิทัลได้อย่างมีประสิทธิภาพ โดยช่วยให้มีสติและรู้เท่าทันข้อมูลที่หลั่งไหลเข้ามาอย่างมหาศาลที่สอนให้คนทั่วไปไม่เชื่ออะไรง่ายๆ ตามหลัก “สาม ก.”ที่ท่านพุทธทาสภิกขุอธิบายเอาไว้ว่า “เหยื่อของโลก” คือ “กิน กาม และเกียรติ” ที่ผู้โจมตีมักจะใช้ความอยากหรือข้อมูลความบันเทิง ความต้องการทางเพศ และความอยากได้เกียรติเป็นเครื่องมือในการหลอกลวง การสร้างภูมิคุ้มกันตามแนวพุทธธรรมไม่ได้จำกัดอยู่แค่การใช้เทคโนโลยีเพื่อป้องกันเท่านั้น หลักพุทธธรรมสอนให้อยู่กับปัจจุบันและรู้เท่าทันอารมณ์ นอกจากนี้ตามหลัก “ปฏิจจสมุปบาท” ในแง่ว่าสิ่งทั้งปวงมีเหตุเกิด มองภัยคุกคามทางเทคโนโลยีในปัจจุบันว่า “ไม่ได้เกิดขึ้นเองอย่างโดดเดี่ยว แต่มีเหตุปัจจัยที่เป็นต้นตอและส่งผลกระทบต่อเนื่องเป็นลูกโซ่” การเข้าใจเหตุและผลของภัยคุกคามจะช่วยให้หาวิธีป้องกันได้อย่างมีประสิทธิภาพ

คำสำคัญ : 1. การประยุกต์; 2. พุทธธรรม; 3. ภัยคุกคามออนไลน์

Abstract

The purpose of this academic article is to study and analyze the application of Buddhist principles in addressing online threats. It is found that digital threats in the present era have become increasingly complex and diverse in line with technological advancements. These threats are designed to deceive or attack targets, constituting a modern form of crime known as cybercrime. Buddhist teachings encourage individuals to apply wisdom and critical thinking, as exemplified in the Kesamutti Sutta or “Kālāma Sutta,” which advises against believing in things too readily. This principle can be effectively applied to digital threats by fostering mindfulness and discernment toward the vast flow of information, thereby

preventing people from believing things uncritically. In this regard, the teaching of Buddhadāsa Bhikkhu on the “Three Prey of the World” (Three Ks: food, sex, and fame) is also relevant. Cyber attackers often exploit human desires such as entertainment, sexual gratification, and the pursuit of prestige as tools of deception. Building immunity through Buddhist principles, therefore, goes beyond mere reliance on technological defenses. Buddhist teachings emphasize living in the present moment and being aware of one’s emotions. Furthermore, the principle of Dependent Origination (Paṭiccasamuppāda) teaches that all phenomena arise from causes and conditions, and do not exist independently. Applying this view, technological threats can be understood as not arising in isolation but as the result of interconnected causes, producing chain reactions of consequences. Understanding the causes and effects of such threats can thus lead to more effective prevention and response.

Keywords: 1. Applying principles; 2. Buddhist; 3. Online Threats

บทนำ

ปัจจุบันการเข้าถึงข้อมูลและการสื่อสารที่ไร้ขีดจำกัดในยุคดิจิทัลได้เปลี่ยนแปลงวิถีชีวิตของผู้คนทั่วโลกอย่างสิ้นเชิง อย่างไรก็ตามโลกออนไลน์ที่กว้างใหญ่นี้ก็เต็มไปด้วยภัยคุกคามหลากหลายรูปแบบ ไม่ว่าจะเป็นข่าวปลอม การกลั่นแกล้งทางไซเบอร์ หรือการหลอกลวงที่นำไปสู่ความเสียหายทั้งทางร่างกายและจิตใจ ปัญหาเหล่านี้ได้สร้างความท้าทายใหม่ที่เกินกว่าจะแก้ไขด้วยมาตรการทางเทคโนโลยีเพียงอย่างเดียว บทความนี้จึงมุ่งศึกษาการประยุกต์ใช้หลัก “พุทธธรรม” ซึ่งเป็นภูมิปัญญาในทางพุทธศาสนาที่มีมายาวนาน เพื่อเป็นแนวทางในการสร้างภูมิคุ้มกันและพัฒนาศักยภาพของพลเมืองดิจิทัลให้สามารถรับมือกับภัยคุกคามออนไลน์ รวมถึงการแทรกแซงทางการเมืองและสงครามข้อมูล ทำให้ความมั่นคงทางไซเบอร์ไม่ใช่เรื่องของบุคคลหรือองค์กรใดองค์กรหนึ่งอีกต่อไป แต่ได้ยกระดับเป็นประเด็นด้านความมั่นคงระดับชาติที่รัฐบาลทั่วโลกต้องให้ความสำคัญอย่างเร่งด่วน ด้วยการตระหนักว่าภัยคุกคามเหล่านี้ไม่ใช่สิ่งที่หลีกเลี่ยงไม่ได้ พลเมืองจึงไม่ควรยอมจำนนต่อกระแสข้อมูลที่ชี้นำ แต่ต้องมีบทบาทในการใช้วิจารณญาณและความรู้เท่าทันสื่อดิจิทัล (วรเจตน์ ภาคีรัตน์, 2561) เพื่อปกป้องสิทธิในการแสดงออกและร่วมกันกำหนดทิศทางของสังคม

บทความนี้จะสำรวจว่าหลักธรรมสำคัญ เช่น สติ (Mindfulness) ปัญญา (Wisdom) หรือหลักพุทธธรรมในพุทธศาสนาสามารถนำมาใช้เป็นเครื่องมือในการรับมือกับความท้าทายในโลกไซเบอร์ได้อย่างไร โดยเฉพาะอย่างยิ่งในแง่ของการพัฒนาการคิดวิเคราะห์อย่างมีเหตุผล การรู้เท่าทันอารมณ์และการใช้ชีวิตในโลกออนไลน์อย่างไม่ประมาท นอกจากนี้จะนำเสนอแนวคิดเชิงบูรณาการเกี่ยวกับการเชื่อมโยงหลักพุทธธรรมเข้ากับแนวทางการสร้างความตระหนักรู้ทางดิจิทัล เพื่อเป็นรากฐานในการสร้างสังคมออนไลน์ที่มีคุณภาพและปลอดภัยยิ่งขึ้น ด้วยการนำเสนอทางเลือกใหม่ที่ไม่ได้พึ่งพิงเพียงเทคโนโลยี แต่เน้นการพัฒนาจิตใจและปัญญาของมนุษย์เป็นสำคัญ

ภัยคุกคามทางดิจิทัลในยุคปัจจุบัน

ภัยคุกคามทางดิจิทัลในยุคปัจจุบันมีความซับซ้อนและหลากหลายมากขึ้นตามการพัฒนาของเทคโนโลยี และผู้ไม่หวังดีที่ใช้วิธีการแนบเนียนปรับเปลี่ยนอยู่เสมอเพื่อหลอกลวงหรือโจมตีเป้าหมายทั้งในระดับบุคคลและองค์กรเป็นอาชญากรรมในยุคใหม่ที่เรียกว่า "อาชญากรรมไซเบอร์" บทความวิชาการของ (วรรณภา ทองแดง, 2563) อธิบายว่าเป็นการกระทำผิดกฎหมายที่ใช้คอมพิวเตอร์และอินเทอร์เน็ตที่ส่งผลกระทบเล็กน้อย เช่น การดาวน์โหลดไฟล์ผิดกฎหมาย ไปจนถึงการโจมตีที่สร้างความเสียหายอย่างรุนแรง เช่น การขโมยเงินจากบัญชีธนาคารออนไลน์ หรือการกระทำที่ไม่ได้มุ่งหวังผลประโยชน์ทางการเงินโดยตรง เช่น การปล่อยไวรัสเพื่อทำลายข้อมูลหรือการเผยแพร่ความลับทางธุรกิจ ภัยคุกคามที่พบบ่อยและน่าสนใจมี ดังนี้

1. Ransomware (มัลแวร์เรียกค่าไถ่)

จากข้อมูลสำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย อธิบายว่า Ransomware Ransomware (แรนซัมแวร์) มัลแวร์ถูกออกแบบมาเพื่อเข้ารหัสไฟล์สำคัญของผู้ใช้ เช่น เอกสาร รูปภาพ หรือวิดีโอเพื่อเรียกค่าไถ่ เมื่อติดเชื้อมัลแวร์จะทำการล็อกไฟล์อย่างรวดเร็ว และแสดงข้อความเรียกค่าไถ่ โดยมักกำหนดให้จ่ายด้วยสกุลเงินดิจิทัลอย่าง "Bitcoin" เพื่อไม่ให้ถูกติดตามได้ง่าย อย่างไรก็ตามไม่มีหลักประกันว่าเมื่อจ่ายเงินแล้วจะได้ข้อมูลคืน ทำให้มัลแวร์เป็นภัยคุกคามที่อันตรายมาก เพราะนอกจากจะสูญเสียข้อมูลแล้ว ยังมีความเสี่ยงที่จะเสียเงินโดยเปล่าประโยชน์อีกด้วย นอกจากนี้มัลแวร์ยังเป็นคำเรียกโดยรวมสำหรับซอฟต์แวร์ประสงค์ร้ายทุกชนิด เช่น ไวรัส โทรจัน และสปายแวร์ ซึ่งแต่ละประเภทมีวิธีการโจมตีที่แตกต่างกันไป

2. Phishing (การหลอกลวงทางอีเมล)

ข้อมูลจากสำนักคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี อธิบายว่า Phishing (ฟิชชิ่ง) คือการหลอกลวงทางอินเทอร์เน็ตที่ผู้ไม่หวังดีจะปลอมแปลงเป็นบุคคลหรือองค์กรที่น่าเชื่อถือ เช่น ธนาคาร บริษัท หรือหน่วยงานภาครัฐ เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัวและข้อมูลทางการเงิน การโจมตีส่วนใหญ่มักจะมาในรูปแบบของอีเมลหรือข้อความที่สร้างความเข้าใจผิดให้เหยื่อทำตาม เช่น คลิกลิงก์เพื่อพาไปยังเว็บไซต์ปลอมที่ดูเหมือนจริงทุกอย่าง เปิดไฟล์แนบที่อาจมีมัลแวร์ซ่อนอยู่และป้อนข้อมูลส่วนตัว เช่น ชื่อผู้ใช้และรหัสผ่าน บนเว็บไซต์ปลอมที่ถูกออกแบบมาเพื่อดักจับข้อมูลโดยเฉพาะ

3. Social Engineering (วิศวกรรมสังคม)

ข้อมูลจาก Kaspersky อธิบายว่า วิศวกรรมสังคม คือการหลอกลวงที่อาศัยจุดอ่อนของมนุษย์ เพื่อขโมยข้อมูลส่วนตัวหรือทรัพย์สินมีค่าต่างๆ การโจมตีลักษณะนี้มักใช้จิตวิทยาในการหลอกล่อให้เหยื่อเปิดเผยข้อมูลสำคัญแพร่กระจายมัลแวร์ หรือให้สิทธิ์เข้าถึงระบบที่ถูกจำกัด โดยอาชญากรไซเบอร์จะใช้ประโยชน์จากพฤติกรรมและความไม่ระมัดระวังของผู้คน รวมถึงความไม่รู้เท่าทันภัยคุกคามทางเทคโนโลยีทำให้การโจมตีแบบนี้มักประสบความสำเร็จ เป้าหมายหลักของนักต้มตุ๋น คือ การทำลายข้อมูล หรือการแสวงหาผลประโยชน์จากทรัพย์สินมีค่า เช่น เงิน ข้อมูล หรือการเข้าถึงระบบต่างๆ

4. ไซเบอร์บูลลี่

จากข้อมูล Unicef อธิบายว่า ไซเบอร์บูลลี่ หรือการกลั่นแกล้งบนโลกออนไลน์ คือการใช้เทคโนโลยีดิจิทัลเพื่อทำร้ายจิตใจผู้อื่นอย่างต่อเนื่องจนเกิดความเจ็บปวด โกรธ หรืออับอายการกระทำเหล่านี้อาจเกิดขึ้นได้หลายรูปแบบ เช่น การโพสต์ข้อมูลเท็จ ภาพ หรือวิดีโอที่น่าอับอายลงบนโซเชียลมีเดีย การส่งข้อความข่มขู่หรือข้อความที่ไม่เหมาะสมผ่านแอปพลิเคชันแชท การปลอมบัญชีเพื่อส่งข้อความทำร้ายจิตใจผู้อื่น สิ่งที่ทำให้

ไซเบอร์บูลลี่แตกต่างจากการกลั่นแกล้งทั่วไปคือ ร่องรอยดิจิทัล (Digital Footprint) ที่ถูกทิ้งไว้ ซึ่งสามารถใช้เป็นหลักฐานในการหยุดยั้งการกระทำดังกล่าวได้

5. การโจมตีแบบ DoS/DDoS

ข้อมูลจาก Akamai อธิบายว่า DDoS (Distributed Denial-of-Service) คือการโจมตีทางไซเบอร์ที่มุ่งเป้าให้เว็บไซต์ เซิร์ฟเวอร์ หรือเครือข่ายหยุดทำงาน โดยการส่งทราฟฟิกปลอมจำนวนมหาศาล เข้าไปโจมตีพร้อมกัน การโจมตีนี้เปรียบเสมือนการจราจรที่ติดขัดอย่างหนักจากการเรียกรถปลอมจำนวนมาก ทำให้รถปกติไม่สามารถวิ่งต่อไปได้ ส่งผลให้ผู้ใช้ทั่วไปไม่สามารถเข้าถึงบริการหรือข้อมูลบนเว็บไซต์ได้ตามปกติ ซึ่งอาจก่อให้เกิดความเสียหายทางการเงินและชื่อเสียงขององค์กรอย่างรุนแรง

การประยุกต์หลักเกสปุตตสูตรกับภัยดิจิทัล

หลัก "กาลามสูตร" เป็นหลักธรรมในพระพุทธศาสนาที่สอนให้คนรู้จักใช้ วิจารณญาณ และไม่ให้เชื่อสิ่งใดโดยง่าย หลักการนี้สามารถนำมาประยุกต์ใช้กับภัยดิจิทัลได้อย่างมีประสิทธิภาพ โดยช่วยให้เรามีสติและรู้เท่าทันข้อมูลที่หลั่งไหลเข้ามาอย่างมหาศาลที่สอนให้ไม่เชื่ออะไรง่ายๆ จนกว่าจะผ่านการพิจารณาด้วยเหตุผลและปัญญา ถือเป็นหัวใจสำคัญในการรับมือกับข้อมูลข่าวสารในโลกออนไลน์ที่เต็มไปด้วยข้อมูลปลอม (Fake News) หรือข่าวลวง และการหลอกลวงในรูปแบบต่างๆ เมื่อนำหลัก "เกสปุตตสูตร" มาประยุกต์ใช้จะสามารถช่วยให้เจาะลึกไปที่การวิเคราะห์ข่าวปลอม โดยใช้หลักการอย่าเพิ่งเชื่อเพราะฟังตามกันมา "มา อนุสฺสเวน" (พระไตรปิฎกฉบับมหามกุฏราชวิทยาลัย, 2544 เล่มที่ 34 ข้อที่ 505 หน้าที่ 338) ในการตรวจสอบความน่าเชื่อถือของแหล่งข่าวการอ้างอิงและความสมเหตุสมผลของเนื้อหา เพราะการจะใช้คำว่า "ถูก" หรือ "ผิด" กับเรื่องใดเรื่องหนึ่งมักมีตัวแปรที่หลากหลายและขึ้นอยู่กับบริบท หรือบางกรณีก็อยู่ภายใต้การตัดสินจากการปฏิบัติตามกฎหรือข้อบังคับที่สังคมกำหนดไว้ เช่น การตัดสินของศาลที่ถูกกฎหมาย หรือเป็นการตัดสินจากความเหมาะสม หรือความเข้ากันได้ตามหลักความงาม เช่น การสร้างภาพลักษณ์ที่ดูดีเกินจริง หรือการเผยแพร่ข้อมูลที่บิดเบือนไปจากความเป็นจริง สิ่งเหล่านี้ทำให้การตัดสินคนทำได้ยากขึ้นและมีโอกาสที่จะผิดพลาดสูง ทำให้คำว่า "ถูก" อาจไม่ได้อาศัยเพียงแบบแผนหรือกฎเกณฑ์ที่สังคมกำหนดขึ้น เพื่อให้สมาชิกในสังคมยึดถือและปฏิบัติร่วมกัน แต่ต้องเป็นเครื่องมือที่มนุษย์ใช้ในการประเมินและตัดสินสิ่งต่างๆ โดยพิจารณาจากความเหมาะสมในแต่ละบริบท ไม่ว่าจะเป็นเรื่องของกฎเกณฑ์ทางศีลธรรม หรือเรื่องของรสนิยมทางสุนทรียศาสตร์ (จำนงค์ ทองประเสริฐ, 2552) เมื่อนำมาวิเคราะห์กับภัยคุกคามทางเทคโนโลยีตามหลัก "สาม ก." ที่ท่านพุทธทาสภิกขุเคยอธิบายเอาไว้ว่า "เหยื่อของโลก" คือ "กิน กาม และเกียรติ" ที่ผู้โจมตีมักจะใช้ความอยากหรือข้อมูลความบันเทิง ความต้องการทางเพศและความอยากได้เกียรติเป็นเครื่องมือในการหลอกลวง ดังนั้นการเข้าใจหลักการนี้อาจจะช่วยให้เรามีสติและรู้เท่าทัน เพื่อไม่ให้ตกเป็นเหยื่อในโลกดิจิทัลได้อีกต่อไปควรทำความเข้าใจหลัก "สาม ก." ดังนี้

1.กิน

ความอยากในข้อมูลข่าวสารและความบันเทิงเปรียบได้กับการ "กินที่ไม่ต้องกิน" เพราะผู้คนเสพข้อมูลเหล่านี้อย่างหิวกระหายโดยไม่ได้ไตร่ตรอง หรือรับข้อมูลที่เกินความจำเป็น การพนันออนไลน์ หรือ เกมที่ต้องเติมเงินไม่สิ้นสุด คือการกินแพงที่ทำให้ผู้คนเสียเงินเป็นจำนวนมากจนเกิดปัญหาหนี้สินการตกเป็นเหยื่อผู้คนหลงใหลในความรวดเร็วและความตื่นเต้นของข้อมูล จนไม่สนใจการตรวจสอบข้อเท็จจริง และยอมจ่ายเงินเพื่อความสุขชั่วคราวทำให้เหมือน "ติดเบ็ด" ในโลกออนไลน์

2.กาม

การใช้ประโยชน์จากความต้องการทางเพศ การหลอกลวงแบบโรแมนติก ผู้โจมตีจะใช้บัญชีปลอมมาตีสนิทและสร้างความสัมพันธ์ เพื่อหลอกลวงให้เหยื่อโอนเงินหรือเปิดเผยข้อมูลส่วนตัว การขู่กรรโชกทางเพศ (Sextortion) หรือ การหลอกให้เปิดกล้อง เพื่อบันทึกภาพและนำมาแบล็กเมล์ ซึ่งเป็นการใช้ประโยชน์จากความอยากทางเพศของเหยื่อโดยตรง สื่อลามกอนาจาร และเว็บไซต์ที่ไม่เหมาะสม ที่แพร่กระจายอย่างง่ายดายในโลกออนไลน์ ล้วนเป็นกับดักที่ทำให้ผู้คนตกเป็นทาสของความต้องการทางเพศ

3.เกียรติ

ความต้องการการยอมรับและการถูก มักใช้หลักการที่กระตุ้นให้เหยื่อรู้สึกอยากได้เกียรติหรือผลประโยชน์ เช่น “คุณได้รับรางวัลใหญ่” หรือ “บัญชีของคุณกำลังจะได้เป็นบุคคลสำคัญ”การสร้างตัวตนปลอม หรือการหลอกลวงเพื่อสร้างเครดิตบนโซเชียลมีเดีย ผู้โจมตีจะสร้างโปรไฟล์ที่ดูดีและน่าเชื่อถือเพื่อหลอกให้เหยื่อไว้วางใจและยอมทำตามการสร้างชื่อเสียงด้วยยอดไลก์และยอดผู้ติดตามปลอม ทำให้ผู้คนยอมทำทุกอย่างเพื่อการยอมรับและคำชื่นชมในโลกออนไลน์ การเข้าใจหลัก “สาม ก.” (พุทธทาสภิกขุ, 2559) จะช่วยให้เรามีสติและรู้เท่าทันภัยดิจิทัล ไม่ตกเป็นเหยื่อของความอยากที่ผู้โจมตีใช้เป็นเครื่องมือในการหลอกลวง

การพัฒนาตามแนวพุทธธรรมเพื่อสร้างภูมิคุ้มกันให้กับตัวเอง

การสร้างภูมิคุ้มกันตามแนวพุทธธรรมไม่ได้จำกัดอยู่แค่การใช้เทคโนโลยีเพื่อป้องกันเท่านั้น แต่ยังรวมถึงการพัฒนาสติและปัญญาของผู้ใช้งานด้วย หลักพุทธธรรมสอนให้อยู่กับปัจจุบันและรู้เท่าทันอารมณ์ ซึ่งมีประโยชน์มากในการใช้งานดิจิทัลสติรู้ทันอารมณ์ และการมีสติช่วยให้ไม่ตอบสนองต่อข้อมูลหรือข่าวที่กระตุ้นอารมณ์โกรธหรือความกลัวได้ในทันที ทำให้มีเวลาไตร่ตรองก่อนที่จะตัดสินใจแชร์หรือแสดงความคิดเห็น ปัญญาในการเลือกรับข้อมูล การพัฒนาปัญญาช่วยให้สามารถแยกแยะระหว่างข้อมูลที่มีประโยชน์กับข้อมูลที่ไร้สาระหรือเป็นอันตรายได้ และเลือกที่จะเสพข้อมูลที่สร้างสรรค์และเป็นประโยชน์ต่อตนเอง ในหนังสือพุทธธรรมของ (สมเด็จพระพุทธโฆษาจารย์, 2562) แนะนำเรื่องของความรู้ที่เนื่องด้วยการปฏิบัติการทางสังคมว่าด้วยเรื่องของความรู้ที่มนุษย์สร้างขึ้นและถ่ายทอดต่อกันมาสามารถจำแนกได้เป็น 3 ประเภทหลัก ได้แก่ สุตตะ ทิฏฐิ, และ ญาณ โดยสามารถอธิบายแต่ละประเภทได้ ดังนี้

1. สุตตะ

ความรู้จากการสดับตรับฟัง หรือการเรียนรู้จากผู้อื่นและจากตำรา เป็นความรู้ที่ถ่ายทอดจากรุ่นสู่รุ่นผ่านการฟัง การบอกเล่า หรือการเรียนรู้จากอาจารย์ เช่น การศึกษาพระไตรปิฎกที่มักขึ้นต้นด้วยคำว่า “เอวัมเม สุตัง” (ข้าพเจ้าได้สดับมาอย่างนี้) เป็นความรู้จากการถ่ายทอดมาโดยตรง ในศาสนาพราหมณ์ความรู้ที่ได้รับจากพระเจ้าโดยตรงจะถูกเรียกว่า “ศรุติ” ซึ่งหมายถึงการฟังจากพระเจ้า ในทางพุทธศาสนาแม้จะไม่มีแนวคิดนี้ แต่ความรู้ที่เกิดจากปัญญาของผู้ที่มีความพิเศษก็ถูกเรียกว่า “สุตตะ” ความรู้ประเภทนี้เน้นที่การรับข้อมูลจากภายนอก ซึ่งเป็นรากฐานสำคัญของการศึกษาและวัฒนธรรม

2. ทิฏฐิ

ความรู้ประเภทนี้ไม่ได้มาจากการสดับฟังเพียงอย่างเดียว แต่เกิดจากการยึดถือและผูกพันกับความคิดเห็นหรือทฤษฎีนั้นๆ อย่างจริงจังจนอาจก่อให้เกิดการรวมกลุ่มหรือการแบ่งฝักแบ่งฝ่าย ลักษณะของทิฏฐิมีรากศัพท์มาจากคำว่า “ทฤษฎี” ในภาษาสันสกฤต หมายถึง ความเชื่อหรือหลักปฏิบัติที่ยึดถือเอาไว้ อาจเป็น

ความเห็นที่เห็นพ้องต้องกัน ทัสสนะ ความถูกใจ (รูจิ) หรือหลักการที่ยึดถือเป็นแนวทาง (ลัทธิ) เป็นความรู้ที่สะท้อนถึงการจัดระเบียบทางความคิดและการปฏิบัติตนในสังคม ซึ่งบางครั้งอาจส่งผลให้เกิดการแบ่งแยกกลุ่มความเชื่ออย่างชัดเจน

3. ญาณ

ความหยั่งรู้ที่มาจากปัญญาภายใน เป็นความรู้ขั้นสูงสุดที่เกิดจากการภาวนา การปฏิบัติ หรือการตรัสรู้ด้วยตนเอง ไม่ได้มาจากการรับข้อมูลจากภายนอกหรือการยึดติดกับทฤษฎีใดๆ เป็นความรู้ที่ลึกซึ้งและเป็นอิสระจากความเชื่อเดิมๆ เปรียบเสมือน "ดวงตา" ที่มองเห็นความจริงของสรรพสิ่งอย่างชัดเจน เป็นความรู้ที่นำไปสู่การเปลี่ยนแปลงขั้นพื้นฐานของชีวิตมนุษย์ ดังเช่น การที่พระพุทธเจ้าทรงบรรลุ สัมมาสัมโพธิญาณ ทำให้เกิดพระพุทธศาสนาขึ้น ซึ่งเป็นความรู้ที่แท้จริงและเป็นประโยชน์ต่อการหลุดพ้นจากทุกข์

นอกจากนี้การวิเคราะห์ภัยคุกคามทางเทคโนโลยีตามหลัก "ปฏิจจสมุปบาท" ในแง่ที่ว่าสิ่งทั้งปวงมีเหตุเกิด โดยการมองภัยคุกคามทางเทคโนโลยีในปัจจุบันว่าไม่ได้เกิดขึ้นเองอย่างโดดเดี่ยว แต่มีเหตุปัจจัยที่เป็นต้นตอและส่งผลกระทบต่อเนื่องเป็นลูกโซ่ การเข้าใจเหตุและผลของภัยคุกคามจะช่วยให้หาวิธีป้องกันได้อย่างมีประสิทธิภาพ เช่น การหลอกลวงออนไลน์และการแฮกข้อมูลไม่ได้เกิดขึ้นโดยไม่มีเหตุผล แต่มีสาเหตุหลักมาจากความประมาทของผู้ใช้ การคลิกลิงก์ที่ไม่น่าเชื่อถือ การดาวน์โหลดไฟล์ที่ไม่รู้จัก หรือการตั้งรหัสผ่านที่คาดเดาง่าย ล้วนเป็นปัจจัยที่ทำให้เกิดช่องโหว่ ผู้โจมตีมีเป้าหมายที่ชัดเจน เช่น การขโมยข้อมูลส่วนตัวเพื่อนำไปขาย การเรียกค่าไถ่ หรือการสร้างความปั่นป่วนทางสังคม รวมถึงช่องโหว่ทางเทคนิค ระบบซอฟต์แวร์หรือแพลตฟอร์มบางอย่างมีข้อบกพร่องด้านความปลอดภัยที่ผู้ไม่หวังดีสามารถใช้เป็นเครื่องมือในการโจมตีได้ หากเข้าใจเหตุที่ทำให้เกิดภัยคุกคาม ก็จะสามารถหาวิธีดับเหตุนั้นได้เช่นกัน นำไปสู่การป้องกันภัยคุกคามทางเทคโนโลยีอย่างยั่งยืน การพัฒนาเทคโนโลยีความปลอดภัย การอัปเดตซอฟต์แวร์อย่างสม่ำเสมอ การติดตั้งโปรแกรมป้องกันไวรัส และการใช้การยืนยันตัวตนแบบหลายขั้นตอน จะช่วยอุดช่องโหว่ทางเทคนิค (วัชระ งามจิตเจริญ, 2556)

การพัฒนาสติปัญญาด้วย "ศาสตร์" และ "พระพุทธศาสนา" จากการที่มนุษย์ขาดความรู้และสติในการรับข้อมูล การรับมือภัยเหล่านี้จึงต้องใช้ทั้งความรู้เชิงวิทยาการและปัญญาทางศาสนา ยกตัวอย่าง ความฉลาดทางปัญญา (Intellectual Intelligence) ในศาสตร์สมัยใหม่ เช่น สังคมศาสตร์และวิทยาศาสตร์ ช่วยให้ฉลาดที่จะเอาตัวเองให้รอด ด้วยการแสวงหาความจริงและสร้างความเข้าใจในโลกแห่งความเป็นจริง การคิดเชิงวิเคราะห์ (Critical Thinking) วิทยาการสอนให้เราตั้งคำถาม เพื่อหาเหตุผลและตรวจสอบข้อมูลอย่างเป็นระบบ และแยกแยะว่าอะไรคือเรื่องจริงและอะไรคือเรื่องหลอกลวง เมื่อนำมาประยุกต์รวมกับคำสอนในพุทธธรรม ในเรื่องความฉลาดทางจิตใจ (Emotional Intelligence) พระพุทธศาสนาเน้นการพัฒนาความรู้ว่าอะไรควรหรือไม่ควร ซึ่งช่วยให้มีสติและรู้เท่าทันอารมณ์ความรู้สึกของตนเองเมื่อต้องเผชิญกับข่าวสารที่กระตุ้นอารมณ์

นอกจากนี้ฐานคิดสำคัญของศาสนาคือ "ศีลธรรม" จะเป็นเครื่องมือในการตัดสินใจว่าสิ่งใดถูกต้องและเป็นประโยชน์ต่อตนเองและผู้อื่น การมีศีลธรรมจะช่วยป้องกันไม่ให้ตกเป็นเครื่องมือของผู้ที่ใช้เทคโนโลยีในทางที่ผิด หลักธรรมในพระพุทธศาสนา เช่น โยนิโสมนสิการ การคิดอย่างมีระบบและการเจริญสติ ช่วยให้มีปัญญาที่จะ "รู้ ตื่น และเบิกบาน" ไม่หลงติดอยู่กับกระแสข้อมูลที่ไร้สาระ (คณาจารย์ มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย, 2563) ดังนั้น การรับมือภัยคุกคามจากเทคโนโลยีจะต้องใช้ทั้งความฉลาดทางปัญญาจาก "ศาสตร์" และความฉลาดทางจิตใจจาก "พระพุทธศาสนา" โดยศาสตร์ช่วยให้มีเครื่องมือในการตรวจสอบ

ข้อมูลและป้องกันภัยทางกายภาพ ขณะที่พระพุทธศาสนาช่วยให้มีสติและศีลธรรมในการเลือกรับและใช้ข้อมูลอย่างถูกต้อง การรวมกันของทั้งสองสิ่งนี้จะสร้างภูมิคุ้มกันทางปัญญาที่สมบูรณ์แบบให้กับมนุษย์ในยุคดิจิทัล

การสร้างภูมิคุ้มกันในระดับสังคม

การนำหลักพุทธปัญญามาใช้ไม่ได้จำกัดอยู่แค่บุคคล แต่สามารถขยายไปสู่การสร้างภูมิคุ้มกันให้กับสังคมในวงกว้างได้ โดยใช้หลักกาลามสูตรเป็นแกนหลัก เพื่อสร้างการรู้เท่าทันให้กับเยาวชนและคนในสังคม การสร้างจริยธรรมดิจิทัล ส่งเสริมการใช้เทคโนโลยีอย่างมีจริยธรรมและมีความรับผิดชอบในสังคม โดยเน้นย้ำถึงผลกระทบของการกระทำบนโลกออนไลน์ที่อาจส่งผลต่อผู้อื่น การศึกษาประเด็นเหล่านี้อย่างลึกซึ้งจะช่วยสร้างสังคมที่รู้เท่าทันภัยดิจิทัลได้อย่างยั่งยืน และมีความสุขสงบอย่างแท้จริงในโลกยุคใหม่ การศึกษาเพื่อสร้างภูมิคุ้มกันทางดิจิทัลการศึกษาในบริบทนี้ไม่ได้จำกัดแค่ระบบโรงเรียน แต่ควรรวมถึงการเรียนรู้ตลอดชีวิต เพื่อให้ประชาชนมีความรู้และทักษะดิจิทัล (digital literacy) ที่จำเป็นในการรับมือกับภัยคุกคามต่างๆ รวมถึงการศึกษาที่ไม่เป็นทางการ (Informal Education) การเรียนรู้ด้วยตัวเองผ่านสื่อออนไลน์ หรือการอบรมระยะสั้นเป็นสิ่งสำคัญ เพราะช่วยให้คนในสังคมตามทันเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว การสร้างทักษะการคิดวิเคราะห์ การสอนให้ประชาชนรู้จักคิดอย่างมีวิจารณญาณ (critical thinking) และประเมินความน่าเชื่อถือของข้อมูล เป็นการลงทุนที่สำคัญที่สุด เพื่อป้องกันการตกเป็นเหยื่อของข่าวปลอมและข้อมูลบิดเบือน แม้จะวัดผลการศึกษาแบบไม่เป็นทางการได้ยาก แต่สามารถประเมินผลลัพธ์ในระดับสังคมได้จากการสังเกตพฤติกรรมอัตราการแชร์ข่าวปลอมที่ลดลง อาจจะเป็นตัวบ่งชี้ให้เห็นว่าสังคมมีความสามารถในการตรวจสอบข้อมูลมากขึ้น คนในสังคมสามารถระบุรูปแบบการหลอกลวงออนไลน์ได้ดีขึ้น จากการมีส่วนร่วมในกิจกรรมดิจิทัลอย่างปลอดภัย เพราะคนในสังคมสามารถใช้เทคโนโลยีอย่างสร้างสรรค์และมีความระมัดระวังมากขึ้น

นอกจากนี้การลงทุนในการศึกษาเพื่อสร้างภูมิคุ้มกันทางดิจิทัลถือเป็นการสร้าง “ทุนมนุษย์ดิจิทัล” (อภิชัย พันธเสน, 2564) ให้กับสังคมที่จะช่วยให้สังคมโดยรวมมีความเข้มแข็งและปลอดภัยมากขึ้นจากภัยคุกคามทางเทคโนโลยี การสร้างความเข้มแข็งทางสังคมนี้เพื่อรับมือกับภัยคุกคามทางเทคโนโลยี เช่น ข่าวปลอม หรือการหลอกลวงออนไลน์ ไม่ใช่การเข้าไปแก้ไขปัญหาให้เพียงอย่างเดียว แต่เป็นการเสริมสร้างพลังให้สังคมสามารถรับมือด้วยตนเองได้ในระยะยาว ควรจัดให้มีนักสังคมสงเคราะห์ด้านดิจิทัลเพื่อให้ข้อมูลที่ถูกต้องแก่ประชาชน ให้ทุกคนมีความเข้าใจที่ตรงกันเกี่ยวกับภัยคุกคามรูปแบบต่างๆ เช่น วิธีสังเกตข่าวปลอมหรือกลโกงออนไลน์ที่สามารถช่วยเหลือผู้ที่ตกเป็นเหยื่อของอาชญากรรมไซเบอร์ได้ โดยการแนะนำช่องทางการแจ้งความ หรือเป็นตัวกลางในการประสานงานกับหน่วยงานที่เกี่ยวข้อง เพื่อให้ผู้ถูกละเมิดได้รับความยุติธรรม สิ่งสำคัญที่สุดคือการกระตุ้นให้บุคคล กลุ่ม หรือชุมชน ตระหนักถึงปัญหาและต้องการที่จะแก้ไขปัญหาด้วยตนเอง การจัดอบรมเชิงปฏิบัติการ หรือการสร้างเครือข่ายภาคประชาชนที่รู้เท่าทันภัยดิจิทัล จะช่วยให้สังคมสามารถป้องกันและแก้ไขปัญหาได้อย่างยั่งยืน โดยไม่ต้องพึ่งพาคนภายนอกเพียงอย่างเดียว (พระมหาจีรวัฒน์ กนฺตวณฺโณ, 2564) การประยุกต์ใช้หลักการเหล่านี้จะเปลี่ยนมุมมองจากการทำงานเพื่อผู้รับบริการ (Work for client) เป็นการทำงานร่วมกับผู้รับบริการ (Work with client) ทำให้เกิดภูมิคุ้มกันทางดิจิทัลที่เข้มแข็งและยั่งยืนในระดับสังคมอย่างแท้จริง

สรุป

ภัยคุกคามทางดิจิทัลในยุคปัจจุบันมีความหลากหลายทั้งมัลแวร์เรียกค่าไถ่ (Ransomware) การหลอกลวงทางอีเมล (Phishing) วิศวกรรมสังคม (Social Engineering) ไซเบอร์บูลลี่ และการโจมตีแบบ DDoS ซึ่งล้วนส่งผลกระทบต่อบุคคลและองค์กรทั้งในด้านข้อมูลทรัพย์สิน และความมั่นคงทางสังคม การรับมือกับภัยเหล่านี้จึงไม่อาจอาศัยเพียงเทคโนโลยี แต่จำเป็นต้องอาศัย สติ ปัญญา ศีลธรรม และหลักคิดจากพุทธธรรมมาประยุกต์ใช้ เช่น หลักเกสปุตตสูตร (กาลามสูตร) ช่วยเสริมวิจารณญาณ ไม่เชื่อสิ่งใดโดยง่าย ส่วนแนวคิด "สาม ก." ของท่านพุทธทาสภิกขุ "กิน กาม เกียรติ" ช่วยให้เข้าใจกลไกการล่อหลอกของอาชญากรไซเบอร์ ขณะเดียวกันการพัฒนาปัญญาตามหลักพุทธธรรมคือ "สุตตะ ทิฏฐิ ญาณ" ตลอดจนการมองภัยตามหลัก "ปฏิจจสมุปบาท" จะทำให้เราเห็นเหตุและผลของปัญหา และสามารถป้องกันได้อย่างยั่งยืน นอกจากนี้การผสานความรู้จากศาสตร์สมัยใหม่ เช่น วิทยาศาสตร์ สังคมศาสตร์ และการคิดเชิงวิเคราะห์ เข้ากับพระพุทธศาสนา การเจริญสติ ศีลธรรม และโยนิโสมนสิการ จะช่วยสร้างภูมิคุ้มกันทั้งในระดับบุคคลและสังคม โดยการศึกษาดิจิทัลอย่างต่อเนื่อง การสร้างจริยธรรมดิจิทัล และการเสริมสร้างเครือข่ายชุมชนที่รู้เท่าทันภัย จะทำให้สังคมไทยก้าวสู่การมี ภูมิคุ้มกันทางดิจิทัลที่มั่นคงและยั่งยืน

ข้อเสนอแนะ

1. การสร้างสติดิจิทัลในระดับหลักสูตร

ควรมีการผลักดันให้หลักการ "กาลามสูตร" และ "โยนิโสมนสิการ" ไม่ได้เป็นเพียงวิชาพระพุทธศาสนา แต่ถูกบูรณาการเข้ากับวิชา "วิทยาการคำนวณ" (Computing Science) ในสถานศึกษา เพื่อให้เด็กและเยาวชนฝึกการหยุดคิดก่อนคลิก โดยใช้สติเป็นตัวกำกับอารมณ์ที่ถูกกระตุ้นจากกลโกงแบบ

2. การประยุกต์ใช้หลัก "ปฏิจจสมุปบาท" ในการออกแบบระบบความปลอดภัย

ในระดับองค์กรหรือนักพัฒนาระบบ ควรนำแนวคิดการมองเหตุปัจจัยต่อเนื่องมาใช้ในการทำ การประเมินความเสี่ยง ไม่มองว่าการโดนแฮกเกิดจากโชคไม่ดี แต่เกิดจาก "วงจรปัจจัย" เช่น (อวิชชา) ความไม่รู้ -> (สังขาร) การตั้งรหัสผ่านง่าย -> (วิญญาณ) การเข้าถึงระบบ -> (นามรูป) ความเสียหายข้อมูล

การตัดวงจรปัจจัย (การดับเหตุ) เช่น การใช้ Multi-Factor Authentication (MFA) เปรียบเสมือนการสร้างข้อต่อที่แข็งแรงไม่ให้วงจรการโจมตีบรรลุผล

3. การเฝ้าระวัง "สาม ก." ในรูปแบบใหม่

หน่วยงานที่เกี่ยวข้องกับการปราบปรามอาชญากรรมทางเทคโนโลยี เช่น พม. หรือ ตำรวจไซเบอร์ ควรจัดทำชุดข้อมูลเตือนภัยที่จัดกลุ่มตามหลัก กิน กาม เกียรติ เพื่อให้ประชาชนจดจำง่าย เช่น การเตือนภัยเรื่องการลงทุนเกินจริง, เว็บพนัน, แอปฯ กู้เงิน เตือนภัยเรื่อง Romance Scam, การแบล็กเมล์ด้วยภาพลับ และเตือนภัยเรื่องการแอบอ้างเป็นเจ้าหน้าที่รัฐ การหลอกว่าได้รับรางวัลใหญ่

4. การสร้างธรรมวิจารณ์ดิจิทัล

ส่งเสริมให้เกิดเครือข่ายภาคประชาชนที่ใช้หลัก "สุตตะ-ทิฏฐิ-ญาณ" ในการคัดกรองข่าวปลอม โดยสนับสนุนกลุ่ม "อาสาสมัครดิจิทัล" ในชุมชน เพื่อทำหน้าที่เปลี่ยนความรู้จากการฟัง (สุตตะ) และความเห็นส่วนตัว (ทิฏฐิ) ให้กลายเป็นความรู้ที่เท่าทันความจริง (ญาณ) เพื่อสื่อสารต่อคนในชุมชนที่เข้าไม่ถึงเทคโนโลยี (เช่น ผู้สูงอายุ)

5. บทบาทของสถาบันทางศาสนาและสังคม

สถาบันสงฆ์หรือผู้นำทางจิตวิญญาณควรปรับบทบาทจากการสอนหลักธรรมในกระดาษ มาเป็นการให้ธรรมะที่เท่าทันโลก เช่น การไม่ไซเบอร์บูลลี่ ไม่บิดเบือนข้อมูล และไม่ละเมิดลิขสิทธิ์ ซึ่งเป็นการสร้าง “หิริโอตตัปปะ” บนโลกออนไลน์ เป็นต้น

ตารางสรุปข้อเสนอแนะในรูปแบบตารางเปรียบเทียบ

ระดับ	มาตรการที่เสนอแนะ	หลักธรรมที่ประยุกต์ใช้
บุคคล	ฝึกสติก่อนโต้ตอบ	กาลามสูตร / โยนิโสมนสิการ
ครอบครัว	สร้างพื้นที่ปลอดภัยพูดคุยเรื่องการถูกบูลลี่หรือหลอกลวง	ศีลธรรม / เมตตาธรรม
องค์กร	วางระบบป้องกันและประเมินความเสี่ยงรายจุด	ปฏิจจสมุปบาท (การดับเหตุ)
สังคม	สร้างเครือข่ายเฝ้าระวังและให้ความรู้ประชาชน	สุตตะ / ญาณ / ทุนมนุษย์ดิจิทัล

เอกสารอ้างอิง

คณาจารย์ มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย. (2563). *ธรรมประยุกต์.* โรงพิมพ์มหาจุฬาลงกรณราชวิทยาลัย.

จำนงค์ ทองประเสริฐ. (2552). *จริยศาสตร์และจริยธรรมเพื่อพัฒนาชีวิตและสังคม.* โรงพิมพ์มหาจุฬาลงกรณราชวิทยาลัย.

พุทธทาสภิกขุ. (2559). *ศิลปแห่งชีวิต.* โรงพิมพ์พระพุทธศาสนาของธรรมสภา.

พระมหาจีรวัฒน์ กนฺตวณฺโณ. (2564). *พระพุทธศาสนากับสังคมสงเคราะห์.* สำนักพิมพ์มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย.

มหามวิทยาลัยมหากุฏราชวิทยาลัย. (2544). *พระไตรปิฎกฉบับมหามกุฏราชวิทยาลัย.* โรงพิมพ์มหามกุฏราชวิทยาลัย.

วัชระ งามจิตเจริญ. (2556). *พุทธศาสนาเถรวาท.* สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

วรเจตน์ ภาคีรัตน์. (2561). *ประวัติศาสตร์ความคิดนิติปรัชญา.* สำนักพิมพ์อ่านกฎหมาย.

วรรณภา ทองแดง. (2563). ผลกระทบเศรษฐกิจดิจิทัล: การขยายตัวของรายจ่ายสาธารณะด้านการศึกษาและภัยคุกคามทางไซเบอร์. *วารสารวิชาการมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยขอนแก่น*. 37(2), 357-358.

สำนักบริหารเทคโนโลยีสารสนเทศ จุฬาลงกรณ์มหาวิทยาลัย. (2536). *Ransomware คืออะไร.* [ออนไลน์]. แหล่งที่มา: https://www.it.chula.ac.th/ransomware.

สมเด็จพระพุทธโฆษาจารย์ (ป.อ. ปยุตฺโต). (2562). *พุทธธรรม ฉบับปรับขยาย.* (พิมพ์ครั้งที่ 52). บริษัท สำนักพิมพ์เพ็ทแอนด์โฮม จำกัด

สำนักคอมพิวเตอร์ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี. (2568). *Phishing คืออะไร ป้องกันมันได้อย่างไร*. [ออนไลน์]. แหล่งที่มา: https://cc.kmutt.ac.th/phishing-mail.html.

อภิชัย พันธเสน. (2564). *พุทธเศรษฐศาสตร์*. (พิมพ์ครั้งที่ 5). สำนักพิมพ์อมรินทร์พริ้นติ้ง แอนด์ พับลิชชิ่ง.

Akamai. (2568). *การโจมตี DDoS คืออะไร*. [ออนไลน์]. แหล่งที่มา: https://www.akamai.com/glossary/what-is-ddos.

Kaspersky. *นิยามของวิศวกรรมสังคม*. (2568). [ออนไลน์]. แหล่งที่มา: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering.

Unicef. (2568). *ไซเบอร์บูลลี่คืออะไร และจะยุติมันได้อย่างไรสิ่งที่วัยรุ่นควรรู้เกี่ยวกับไซเบอร์บูลลี่*. [ออนไลน์]. แหล่งที่มา: https://www.unicef.org/thailand/th/stories.