

บทความวิชาการ

การสร้างวัฒนธรรมไซเบอร์เชิงบวก

สำหรับนักศึกษาระดับปริญญาตรี

ณลินี จรรยาพัฒนานนท์¹ และอติป แทนรัตนกุล²

Received 22 February 2024

Revises 26 March 2024

Accepted 28 March 2024

บทคัดย่อ

การใช้สื่อออนไลน์ในยุคไซเบอร์มีความสำคัญอย่างมาก การสร้างวัฒนธรรมไซเบอร์ จึงเป็นพื้นฐานสำคัญเพื่อช่วยให้มีความรู้ ความเข้าใจ วิเคราะห์ และปรับตัวให้เข้ากับโลกออนไลน์ที่มีอิทธิพลและบทบาทสำคัญต่อวิถีชีวิตของมนุษย์ รวมถึงการใช้ชีวิตประจำวัน การสร้างวัฒนธรรมไซเบอร์เชิงบวก มีส่วนสำคัญในการลดปัญหาที่เกิดขึ้นจากการใช้สื่อออนไลน์ เช่น การส่งเมลหลอกลวง การกระทำความผิดกฎหมายทางไซเบอร์ การละเมิดหรือหมิ่นประมาทผ่านระบบคอมพิวเตอร์ การเปิดเผยข้อมูลส่วนบุคคล การหลอกลวงให้โอนเงิน หรือหลอกลวงให้หลงรัก ซึ่งการกระทำดังกล่าวส่งผลกระทบให้เกิดความสูญเสียต่อทรัพย์สินและความรู้สึกของผู้ถูกกระทำเป็นอย่างมาก

¹ ดร., มหาวิทยาลัยบูรพา, E-mail : priw_nalinee@hotmail.com

² ดร., นักวิชาการอิสระ, E-mail : nineatip@hotmail.com



ดังนั้น การสร้างความวัฒนธรรมไซเบอร์ในเชิงบวกกับกลุ่มนักศึกษาจะเป็นส่วนหนึ่งในการลดและป้องกันปัญหาที่เกิดขึ้น รวมถึงการรู้เท่าทันต่อภัยคุกคามทางไซเบอร์ต่าง ๆ ซึ่งส่วนสำคัญที่เกี่ยวข้อง ได้แก่ การสร้างความและส่งเสริมให้มีจิตสำนึกที่ดีในการมีส่วนร่วมในการเสริมสร้างวัฒนธรรมไซเบอร์เชิงบวก เพราะในปัจจุบัน ใช้เวลาอยู่กับคอมพิวเตอร์และไซเบอร์ทุกวัน ถ้าวัยเด็กและเยาวชน หลงกระทำผิดทางไซเบอร์จะถูกลงโทษเช่นเดียวกับผู้ใหญ่ที่พนินิติภาวะแล้ว จึงควรมีแนวทางเพื่อชะลอหรืออาจจะหยุดการกระทำผิดทางไซเบอร์ของนักศึกษา นอกจากการใช้กฎหมายในการกำกับดูแล การให้ความรู้ และถ่ายทอดวิธีการรับมือกับปัญหาอย่างเหมาะสม

คำสำคัญ: การสร้างวัฒนธรรม, วัฒนธรรมไซเบอร์, นักศึกษาระดับปริญญาตรี,
การแพร่กระจาย

Benefits of Creating a Positive Cyber Culture for Undergraduate Students

Nalinee Junyawattananon³ and Atip Tanrattanakul⁴

Abstract

The use of online media in the cyber age is extremely important. Creating Cyberculture, therefore, is an important basis to help have knowledge, understanding, analysis, and adaptation to the online world that has an important influence and role on human life in daily life. Creating positive cyberculture plays an important role in reducing problems that arise from online media use, such as sending fraudulent emails, cybercrime offenses, infringement, defamation through a computer system, disclosure of personal information money transfer scams, or deception into falling in love. This action has greatly affected the loss of property and feelings of the injured person.

³ Burapha University E-mail: priw_nalinee@hotmail.com

⁴ Independent Scholar E-mail: nineatip@hotmail.com

Therefore, creating a positive cyberculture among students. It will be a part of reducing and preventing problems that occur. Including being aware of various cyber threats, which is an important part involved in creating awareness and encouraging a good conscience to participate in fostering a positive cyberculture.

Keywords: Cyber hygiene culture, Cyberculture, Undergraduate Students, Diffusion



บทนำ

ไซเบอร์ มีความหมายถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการ หรือประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือเครือข่าย โทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่ คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป (Cyber Security Maintenance ACT, B.E. 2019, 2019) โดยในช่วงปี พ.ศ. 2566 หลังจากวิกฤติโควิด-19 ส่งผล ให้รูปแบบการใช้ชีวิตเปลี่ยนแปลงไป ประชาชนคุ้นชินกับการใช้เทคโนโลยี เกิด บริการใหม่ ๆ ที่ใช้แพลตฟอร์มการบริการดิจิทัลที่หลากหลาย โดยถือเป็น จุดเริ่มต้นของการใช้ชีวิต การบริโภค และการดำเนินธุรกิจแบบ New normal จากผลสำรวจมีผู้ใช้อินเทอร์เน็ต 58.3 ล้านคน (ร้อยละ 88.5) ใช้โทรศัพท์มือถือ 62.6 ล้านคน (ร้อยละ 95.1) และมีโทรศัพท์มือถือ 58.0 ล้านคน (ร้อยละ 88.2) ในช่วงไตรมาสที่ 3 ของปี พ.ศ. 2566 จำนวนผู้ใช้โทรศัพท์มือถือมีเพิ่มมากขึ้น (National Statistical Office Thailand, 2023) ในปัจจุบัน “ไซเบอร์” (Cyber) เป็นคำที่ถูกกล่าวถึงอย่างมาก หากนำคำว่า “Cyber” นำหน้าคำอื่น หมายถึง คอมพิวเตอร์หรืออิเล็กทรอนิกส์ รวมทั้งระบบอินเทอร์เน็ตที่เชื่อมต่อ เช่น Cyberbullying แปลว่า การกระรานทางระบบการสื่อสารที่ผ่าน คอมพิวเตอร์ เช่น Facebook, X (Twitter) Cybercrime แปลว่า อาชญากรรม ทางคอมพิวเตอร์ Cybersex แปลว่า การสื่อสารผ่านคอมพิวเตอร์โดย จุดประสงค์เรื่องทางเพศ Cyberporn แปลว่า ภาพโป๊ที่ส่งมาทางคอมพิวเตอร์ Cyberpunk แปลว่า ผู้ที่ใช้คอมพิวเตอร์ไปก่ออาชญากรรมต่าง ๆ (Longdo Dict, 2008)



สถิติภัยคุกคามทางไซเบอร์ในช่วง พ.ศ. 2564-2566 พบว่า ตั้งแต่ปี พ.ศ. 2564 ถึงไตรมาสแรกของปี พ.ศ. 2566 ภาคการผลิตได้รับการจัดอันดับให้เป็นเป้าหมายสูงสุดสำหรับการโจมตีด้วยมัลแวร์อย่างต่อเนื่องทั่วโลก (ThaiCERT, 2023) โดยรูปแบบการโจมตีทางไซเบอร์ที่พบในธุรกิจ SME ของไทย จากผลการวิจัยของ Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense by Cisco พบว่า ธุรกิจในประเทศไทยโดยประมาณ ร้อยละ 56 ได้ประสบปัญหาการดำเนินงานหยุดชะงักเนื่องจากการโจมตีทางไซเบอร์ และร้อยละ 47 ที่เคยถูกโจมตีสร้างความเสียหายต่อธุรกิจคิดเป็นมูลค่าอย่างน้อย 16 ล้านบาท ขณะที่ร้อยละ 28 ได้รับความเสียหายเป็นมูลค่ากว่า 32 ล้านบาท ซึ่งสาเหตุสำคัญที่สุดที่ทำให้ ร้อยละ 49 ของธุรกิจ SME ถูกโจมตีจากการโจมตีด้วยมัลแวร์มาเป็นอันดับหนึ่ง (ร้อยละ 91) และตามด้วยการโจมตีในรูปแบบฟิชชิ่ง (Phishing) มากถึงร้อยละ 77 เนื่องจากว่าโซลูชันด้าน Cybersecurity ไม่มีประสิทธิภาพเพียงพอที่จะตรวจจับ หรือป้องกันการโจมตีจากภัยคุกคามทางไซเบอร์ได้ ในขณะที่ ร้อยละ 25 ระบุว่าสาเหตุหลักคือองค์กรนั้น ๆ ไม่ได้ติดตั้งโซลูชันด้าน Cybersecurity และไม่ได้ให้ความสำคัญด้านความปลอดภัยเป็นอันดับแรก ๆ และในรายงานผลวิจัยข้างต้นยังระบุว่า มีจำนวน ร้อยละ 76 ของบริษัทที่ถูกโจมตีสูญเสียข้อมูลของลูกค้าไป และร้อยละ 69 ของบริษัทได้สูญเสียข้อมูลของพนักงาน อีกทั้ง ยังมีบริษัทที่ถูกโจมตีคิดเป็นอัตราส่วนที่แตกต่างกันไปได้มีการสูญเสียข้อมูลอีเมลภายในองค์กร (ร้อยละ 65) สูญเสียทรัพย์สินทางปัญญา (ร้อยละ 53) สูญเสียข้อมูลด้านการเงิน (ร้อยละ 57) และสูญเสียข้อมูลธุรกิจที่สำคัญอื่น ๆ (ร้อยละ 49) ซึ่งการถูกโจมตีทางไซเบอร์กว่าร้อยละ 80 ส่วนใหญ่เกิดจากความผิดพลาดของมนุษย์ ดังนั้น หาก



เจ้าของธุรกิจต้องการที่จะอุดช่องโหว่ไม่ให้เกิดรอยร้าวให้บรรดาแฮกเกอร์เข้ามาโจมตีได้นั้น การให้ความรู้เกี่ยวกับการรักษาความปลอดภัยทางข้อมูลแก่บุคลากรในองค์กร จึงเป็นสิ่งสำคัญที่จำเป็นจะต้องทำควบคู่กันไปกับการดูแลและตรวจสอบระบบ (NT Cyfence, 2022)

ธนาคารแห่งประเทศไทย (Bank of Thailand, 2023) ได้กล่าวถึงภัยไซเบอร์ในปัจจุบันที่สถาบันการเงิน ภาคธุรกิจต่าง ๆ หรือหน่วยงานภาครัฐถูกโจมตี แบ่งเป็น 3 ประเภท คือ 1) มิจฉาชีพบน Social media โดยนำข้อมูลจากแชทหรือโพสต์ต่าง ๆ เป็นตัวช่วยในการสวมรอยหรือปลอมแปลงข้อมูลเพื่อหลอกลวงประชาชน เช่น การส่งข้อความแชทเพื่อหลอกให้โอนเงิน หรือการปลอมแปลงสลิปโอนเงินในการสั่งซื้อสินค้าออนไลน์ 2) อีเมลล์หลอกลวง (Phishing) จะทำส่งอีเมลล์โดยการแอบอ้างเป็นธนาคารพาณิชย์ เพื่อหลอกให้ทำธุรกรรม หรือกรอกข้อมูลสำคัญ เช่น รหัสผ่าน หมายเลขบัตรเครดิต และยังฝังมัลแวร์ (โปรแกรมมุ่งร้าย) ไว้ในเอกสารแนบของอีเมลล์ เมื่อเปิดไฟล์ดังกล่าวจะทำให้เครื่องคอมพิวเตอร์ของผู้รับได้รับความเสียหาย 3) การขโมยข้อมูลส่วนบุคคล (Data theft) เกิดจากการถูกแฮกข้อมูล หรือทำข้อมูลรั่วไหลจากเว็บไซต์และบริการสาธารณะที่ประชาชนส่วนใหญ่ใช้งานอยู่ เช่น ชื่อบัญชีผู้ใช้งาน รหัสผ่าน หรือข้อมูลบัตรเครดิต และมิจฉาชีพสามารถใช้ข้อมูลดังกล่าวเข้าถึงบัญชีผู้ใช้งานของเราหรือกระทำการใดโดยมิชอบในนามของเราได้ รวมถึงภัยทางไซเบอร์ที่เกิดจากการหลอกลวงว่ามาจากสถาบันทางการเงิน หรือหน่วยงานภาครัฐและเอกชนในการหลอกให้โอนเงินหรือจ่ายเงิน เช่น ได้รับคืนภาษี คืนค่าน้ำ ค่าไฟ การสำรวจที่ดิน การได้รับโปรโมชั่นจากสินค้า หรือได้รับแจกจาก



หน่วยงานที่ถูกพาดพิง ซึ่งสาเหตุส่วนใหญ่จะเกิดจากข้อมูลรั่วไหลจากหน่วยงาน หรือมีการละเมิดข้อมูลของผู้เสียหาย เหล่านี้ก่อให้เกิดผลกระทบต่อผู้เสียหาย ซึ่งเหล่านี้ก่อให้เกิดผลกระทบต่อผู้เสียหายเป็นจำนวนมากศาล และบางรายส่งผลกระทบต่อชีวิตของผู้ได้รับผลกระทบอย่างที่เคยเกิดขึ้น

ปัจจุบันประเทศไทยได้ออกกฎหมายกำกับดูแล และควบคุมการใช้คอมพิวเตอร์ การใช้อินเทอร์เน็ตในรูปแบบต่าง ๆ ที่คุกคามผู้อื่น โดยกฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ จัดทำขึ้นเพื่อป้องกันและให้ความร่วมมือในการรับมือกับภัยคุกคามที่เกิดขึ้นในระบบคอมพิวเตอร์ หรือระบบเทคโนโลยีสารสนเทศ (Kongboonma, 2019) จำนวนหลายฉบับ และมีบทลงโทษชัดเจน เช่น พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และแก้ไขเพิ่มเติม พ.ศ. 2560 ที่เป็นกฎหมายหลักในการกำกับดูแลอินเทอร์เน็ตที่มีความรับผิดชอบทางอาญา พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากเครือข่ายคอมพิวเตอร์ อินเทอร์เน็ต โครงข่ายโทรคมนาคม หรือการให้บริการของดาวเทียม พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 สำหรับกำหนดวิธีการการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดสิทธิความเป็นส่วนตัวไม่ให้เกิดความเดือดร้อน รำคาญ หรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกาศคณะกรรมการกำกับดูแลด้านความปลอดภัยไซเบอร์ พ.ศ. 2566 ที่กำหนดลักษณะของภัยคุกคามทางไซเบอร์ เป็น 3 ระดับ คือ ภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง ระดับร้ายแรง และในระดับวิกฤติ เพื่อให้หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานแจ้งเหตุคุกคามทาง



ไซเบอร์ที่อยู่ในความรับผิดชอบของหน่วยงาน เป็นต้น ซึ่งกฎหมายแต่ละฉบับมุ่งหวังที่จะหยุดการคุกคามทางไซเบอร์ และการกระทำผิดทางไซเบอร์ จึงมีการเพิ่มบทลงโทษ เพิ่มขึ้นตามสถานการณ์ที่รุนแรงขึ้น

นักศึกษาในระดับปริญญาตรีถือเป็นกลุ่มคนเริ่มต้นสำคัญที่จะทำให้เกิดวัฒนธรรมไซเบอร์เชิงบวก เนื่องจากเป็นวัยที่มีความต้องการเรียนรู้สิ่งใหม่ ๆ โดยเฉพาะทางด้านเทคโนโลยีสารสนเทศ และเป็นกลุ่มที่มีโอกาสเสี่ยงสูงที่จะกระทำผิด หรือถูกชักชวนให้กระทำผิดทางไซเบอร์ มหาวิทยาลัยจึงเป็นส่วนในการเตรียมความพร้อมการพัฒนาทักษะของนักศึกษา และเป็นการวางแผนในระยะยาวด้านบุคลากรด้านวัฒนธรรมไซเบอร์

ดังนั้น การให้การศึกษาในระดับอุดมศึกษาทางด้านวัฒนธรรมไซเบอร์เชิงบวกกับนักศึกษาถือเป็นส่วนสำคัญในการชะลอหรืออาจจะหยุดการกระทำผิดทางไซเบอร์ของนักศึกษาได้นอกจากการใช้กฎหมายในการกำกับดูแลคือ การให้ความรู้ ซึ่งพบว่า นักศึกษามหาวิทยาลัยมีคะแนนวัดความรู้ด้านการกระทำผิด และการป้องกันการกระทำผิดน้อยกว่านักศึกษาระดับมัธยมในพื้นที่ภาคเหนือ ซึ่งโรงเรียนมีการให้ความรู้และถ่ายทอดวิธีการรับมือกับปัญหาอย่างเหมาะสม (Thumronglaohapun et al., 2022) การรังแกกันผ่านโลกไซเบอร์ในสตรี เด็ก และเยาวชนเป็นปัญหาที่เกิดผลกระทบต่อเยาวชนที่เป็นอนาคตของชาติ เพราะสามารถแพร่กระจายการรับรู้ไปสู่บุคคลอื่น ๆ ได้อย่างรวดเร็วและก่อให้เกิดผลกระทบในวงกว้าง และเป็นระยะเวลาที่ยาวนานไม่มีที่สิ้นสุด อีกทั้งการกลั่นแกล้งบางประเภทยังไม่มีบทลงโทษทางกฎหมาย เช่น การรังแกด้วยข้อความเท็จหรือลามก การล้อเลียน การติดตามรังควาน การกล่าวถึงโดยการใช้อิ



อักษรย่อ แต่สังคมสามารถรับรู้ได้ หรือทำให้เกิดความเข้าใจผิด เป็นต้น (The National Broadcasting and Telecommunication Commission, 2022)

การถูกรังแกผ่านโลกไซเบอร์ส่งผลต่อสภาพจิตใจ อารมณ์ และคุณภาพชีวิตที่ส่งผลให้เกิดความรุนแรง ความเครียด จนถึงขั้นพยายามฆ่าตัวตาย เพื่อให้หลุดพ้นจากความเครียดและความทรมานที่ได้รับ เช่น 1) การถูกนินทา ด่าทอ รวมถึงการพุดคุยโต้ตอบด้วยถ้อยคำที่หยาบคายผ่านโลกไซเบอร์ 2) การถูกหมิ่นประมาท 3) การถูกแอบอ้างชื่อในด้านลบ 4) การถูกบุคคลอื่นนำความลับที่เป็นข้อมูลส่วนตัวไปเปิดเผย 5) การถูกลบหรือบล็อกจากกลุ่ม ซึ่งการกระทำดังกล่าวมีผลกระทบต่อจิตใจ ร่างกาย และความสัมพันธ์ทางสังคม (Chainwong, Skulphan, & Thapinta, 2020) ซึ่งปัญหาการถูกระรานทางไซเบอร์เป็นภัยเงียบที่เกิดจากความอึดอัด และไม่ได้คำนึงถึงผลกระทบที่เกิดขึ้นในภายหลัง ซึ่งพฤติกรรมของเยาวชนกลุ่มมัธยมศึกษา กับระดับมหาวิทยาลัยมีความแตกต่างกันทั้งในช่วงอายุและการแสดงพฤติกรรม (Tawekanachot, 2022) เยาวชนในช่วงอายุระดับอุดมศึกษา เป็นกลุ่มที่มีโอกาส ศักยภาพ รวมถึงรูปแบบการดำรงชีวิตประจำวันที่มีความต้องการในการเข้าถึงโลกไซเบอร์อย่างมีประสิทธิภาพสูงมาก จนส่งผลให้มีแนวโน้มที่จะตกเป็นเหยื่อหรือเป็นผู้ริเริ่มปัญหาการรังแกกันผ่านโลกไซเบอร์ หรือการใช้ระบบอินเทอร์เน็ตเป็นเครื่องมือในการทำร้ายบุคคลอื่น เพราะมีทัศนคติที่ถูกบ่มเพาะหรือพัฒนาขึ้นมาด้วยประสบการณ์การเรียนรู้ในเชิงลบ ปราศจากการขัดเกลาด้วยความเอาใจใส่ ตั้งแต่ในวัยเด็ก จนส่งผลให้มองการรังแกกันผ่านโลกไซเบอร์เป็นเรื่องปกติทั่วไป และกลายเป็นส่วนหนึ่งของจิตใจ จึงแสดงทัศนคติดังกล่าวผ่านโลกไซเบอร์



เพราะสามารถเข้าถึงได้ง่าย และสามารถตอบสนองความ
พึงพอใจหรือความต้องการของตนเองได้ (The National Broadcasting and
Telecommunication Commission, 2022) ดังนั้น การสร้างวัฒนธรรมการ
ใช้ไซเบอร์ในเชิงบวกให้แก่นักศึกษา เพื่อนำไปใช้ในชีวิตประจำวันสำหรับสื่อสาร
กันผ่านอินเทอร์เน็ต ก่อให้เกิดการดำเนินชีวิตที่มีเทคโนโลยีเป็นกลไก และเป็น
การสร้างวัฒนธรรมที่พัฒนามาจากการใช้เทคโนโลยีการสื่อสารร่วมกัน (Office
of the Royal Society, 2020) เพราะวัฒนธรรมเป็นสิ่งที่ฝังลึก และสะท้อน
การปฏิบัติที่เป็นระเบียบเรียบร้อย และศีลธรรมที่ดั่งาม บทความฉบับนี้จึงเขียน
เชิงวิเคราะห์และการนำเสนอในประเด็นประโยชน์ของการสร้างวัฒนธรรม
ไซเบอร์เชิงบวกสำหรับนักศึกษาระดับปริญญาตรี เพื่อใช้เป็นแนวทางในการใช้
สื่อออนไลน์ที่ถูกต้องและลดความเสี่ยงที่จะเกิดภัยจากไซเบอร์

รูปแบบการสื่อสารที่ใช้ระบบไซเบอร์

โลกไซเบอร์ (Cyberworlds) คือ โลกของสารสนเทศ ซึ่งเป็นได้ทั้งโลก
เสมือนจริง โลกจริง หรือโลกที่ผสมกันระหว่างความเป็นจริงและสารสนเทศ
เสมือน (Wikipedia, 2020) ซึ่งสารสนเทศในยุคปัจจุบันจะเป็นสื่อสังคม
ออนไลน์ เพื่อใช้ในการสื่อสารระหว่างกันในเครือข่ายทางสังคม (Social
Network) ผ่านทางเว็บไซต์ และโปรแกรมประยุกต์บนสื่อใด ๆ ที่มีการเชื่อมต่อ
กับอินเทอร์เน็ต โดยเน้นให้ผู้ใช้ทั้งที่เป็นผู้ส่งสาร และผู้รับสารมีส่วนร่วม
(Collaborative) อย่างสร้างสรรค์ ในการผลิตเนื้อหาขึ้นเองในรูปของข้อมูล
ภาพ และเสียง โดยสามารถแบ่งกลุ่มหลัก ๆ คือ 1) Weblogs หรือเรียกสั้น ๆ
ว่า Blogs คือ สื่อส่วนบุคคลบนอินเทอร์เน็ตที่ใช้เผยแพร่ข้อมูล ข่าวสาร ความรู้



ข้อคิดเห็น บันทึกร่วมกัน โดยสามารถแบ่งปันให้บุคคลอื่น ๆ โดยผู้รับสารสามารถเข้าไปอ่าน หรือแสดงความคิดเห็นเพิ่มเติมได้ เช่น Seasons in Color เป็นเว็บไซต์ที่แบ่งหมวดหมู่แต่ละบล็อกเกอร์ไว้ หรือ Simply Tabitha เป็นตัวอย่างการสร้างบล็อกไลฟ์สไตล์ 2) Social Networking หรือเครือข่ายทางสังคมในอินเทอร์เน็ต ซึ่งเป็นเครือข่ายทางสังคมที่ใช้ สำหรับเชื่อมต่อระหว่างบุคคล กลุ่มบุคคล เพื่อให้เกิดเป็นกลุ่มสังคม (Social Community) เพื่อร่วมกันแลกเปลี่ยนและแบ่งปันข้อมูลระหว่างกันทั้งด้านธุรกิจ การเมือง การศึกษา เช่น Facebook, MySpace, YouTube, Instagram, Line, X (Twister), ฯลฯ (Faculty of Science and Technology Dhonburi Rajabhat University, 2019) โดย Matanboon (2022) พบว่า โซเชียลมีเดียซึ่งเป็นส่วนหนึ่งของ Cyber ทำให้คนเกลียดชังกันได้ โดยการถกเถียงหรือทะเลาะกันในโซเชียลมีเดียส่งผลให้บันดาลโทสะ และผลเสียต่าง ๆ ตามมา เนื่องจากใช้เวลาว่างในการฟังเพลงหรือดูหนังแนวผจญภัย เล่นเกมส์ต่อสู้ เช่น Thairath (2024) ลงข่าวว่า “แก๊งค์โจป็นดู ชีจักรยานยนต์ล่าอริ ยิ่งกันตาย เพราะท้าทายผ่านโซเชียล ทำให้คนบาดเจ็บ 2 คน และเสียชีวิต 1 คน”

ปัจจัยที่มีผลต่อการรับรู้การใช้งานง่ายของคอมพิวเตอร์ และระบบอินเทอร์เน็ต

ปัจจุบันมีการใช้คอมพิวเตอร์กันอย่างกว้างขวางและจำนวนมาก อีกทั้งรัฐบาลประเทศต่าง ๆ พยายามนำคอมพิวเตอร์และอินเทอร์เน็ตมาทำงานด้านการบริการ การเก็บข้อมูล การเรียกหาข้อมูล การสื่อสาร และติดตามประมวลผล วิเคราะห์ผลต่าง ๆ แม้แต่ประเทศไทยได้พัฒนาให้เกิดเมืองอัจฉริยะ



หรือ Smart City โดยมีงบประมาณสนับสนุนระบบอินเทอร์เน็ตและการติดต่อกับราชการให้มีการใช้ผ่านระบบอินเทอร์เน็ต ควบคู่ไปกับการบริการของเจ้าหน้าที่ (Digital Economy Promotion Agency, 2019)

เมื่อมาพิจารณาว่าเหตุใดการติดต่อสื่อสาร การเก็บข้อมูล การประมวลผลข้อมูลที่นิยมใช้ระบบเชื่อมต่อของคอมพิวเตอร์กับอินเทอร์เน็ต จึงเป็นที่นิยมมาก อาจจะเป็นเพราะในปัจจุบันคนได้เรียนรู้การใช้งาน มีการเรียนรู้การพัฒนาให้คนใช้งานง่ายขึ้น เหมือนอุปกรณ์ทั่วไปไม่ใช่สิ่งลึกลับ ดังที่ Venkatesh and Bala (2008) ได้ค้นพบและสรุปไว้ว่า ปัจจุบันคอมพิวเตอร์ระบบอินเทอร์เน็ตสามารถเข้าถึงง่าย ใช้งานง่าย มีสาเหตุปัจจัยมาจาก 1) คนมีความสามารถด้านคอมพิวเตอร์มากขึ้น 2) คนใช้มีการรับรู้ว่ามีควบคุมจากภายนอกที่ช่วยติดตาม 3) ความวิตกกังวลต่อระบบคอมพิวเตอร์ลดลง 4) ความสนุกสนานที่ได้จากระบบคอมพิวเตอร์ 5) ระบบทำให้ใช้งานง่ายขึ้นมาก 6) คอมพิวเตอร์นำมาซึ่งความเพลิดเพลิน 7) สามารถนำคอมพิวเตอร์และระบบอินเทอร์เน็ตไปใช้ประโยชน์ตามต้องการได้ เมื่อมีคนกลุ่มหนึ่งรับรู้ และปฏิบัติได้ ก็จะแพร่กระจาย แนวคิดการปฏิบัติไปยังกลุ่มอื่น ๆ อย่างไม่หยุดยั้ง สอดคล้องกับทฤษฎีการแพร่กระจายนวัตกรรม

ทฤษฎีการแพร่กระจายนวัตกรรม

สังคมไซเบอร์จะเป็นโลกเสมือนจริง (Virtual world) ที่เกิดจากการติดต่อสื่อสารระหว่างผู้ใช้งานในแต่ละสังคมทั่วโลกด้วยระบบอินเทอร์เน็ต ซึ่งลักษณะที่แท้จริงของสังคมไซเบอร์เป็นสังคมที่รวมระหว่างระบบผู้ใช้งานและอุปกรณ์ต่าง ๆ หรือเรียกว่าระบบสังคมเทคโนโลยี (Socio-Technical



System) (Sangsuriyong, 2021) ถือเป็นนวัตกรรมที่ได้รับจากการเปลี่ยนแปลงตามยุคสมัย ที่สามารถเปลี่ยนแปลงสังคมและวัฒนธรรมที่เกิดขึ้น เนื่องจากการแพร่กระจายของสิ่งใหม่ ๆ จากรูปแบบหนึ่งไปสู่อีกรูปแบบหนึ่ง และสังคมนั้น ๆ ได้นำรูปแบบนั้นไปปรับใช้ โดยการแพร่กระจายนวัตกรรมมีองค์ประกอบที่สำคัญ คือ 1) นวัตกรรม 2) การสื่อสารโดยผ่านสื่อทางใดทางหนึ่ง 3) เกิดในช่วงเวลาใดเวลาหนึ่ง 4) ระบบสังคม (Social system) (Everett, 1995)

เทคโนโลยีที่มีการพัฒนาไปอย่างรวดเร็ว และแหล่งข้อมูลที่มหาศาลส่งผลให้การสื่อสารผ่านอินเทอร์เน็ตที่สามารถเชื่อมต่อกันได้ทั่วโลก เป็นจุดเริ่มต้นของความคิดสร้างสรรค์ การเปลี่ยนแปลง และนวัตกรรมต่าง ๆ เพื่อให้มีความตื่นตัวในยุคดิจิทัล (Office of the National Anti-Corruption Commission, 2021) โดยนวัตกรรมที่เกิดจากคอมพิวเตอร์และอินเทอร์เน็ตเมื่อใช้แล้วเกิดประโยชน์ในด้านการติดต่อสื่อสาร ค้นคว้า ประมวลผล และส่งผลให้สามารถกำเนิดอาชีพ และเศรษฐกิจได้ ก็จะมีการแพร่กระจายในลักษณะแพร่กระจายความสามารถของคอมพิวเตอร์และระบบอินเทอร์เน็ตว่ามีศักยภาพซึ่งสอดคล้องกับทฤษฎีศักยภาพในการพัฒนาและการแพร่กระจาย (Development Potential Diffusion Theory) และการแพร่กระจายจะเกิดได้เร็วหากการแพร่กระจายนั้นทำให้เกิดรายได้ (Sunyawiwat, 2007) คอมพิวเตอร์และระบบอินเทอร์เน็ตได้เร็วขึ้น และทำให้เกิดนวัตกรรมใหม่ ๆ ตลอด ทำให้เกิดการแพร่กระจายได้เร็วขึ้นด้วยนวัตกรรมที่ใคร ๆ ก็กล่าวถึงคำว่า นวัตกรรม จากคอมพิวเตอร์และระบบอินเทอร์เน็ต สอดคล้องกับ ทฤษฎีการแพร่กระจายนวัตกรรม (The Diffusion Of Innovation Theory) ของ



Rogers (2003, pp. 11-15) โดยมีหลักว่าการแพร่กระจายนวัตกรรมมีองค์ประกอบสำคัญ คือ 1) นวัตกรรม 2) การสื่อสารนวัตกรรมออกไปให้คนรับรู้ 3) เกิดในช่วงเวลาหนึ่ง 4) เผยแพร่เข้าสู่ชุมชนหนึ่งแล้วไปยังชุมชนอื่น ๆ

ภัยคุกคามทางไซเบอร์

Matrakool and lamviriyakul (2018) ได้สรุปข้อมูลในนามศูนย์ข้อมูลข่าวสารอิเล็กทรอนิกส์ ธนาคารแห่งประเทศไทยว่า ปัจจุบันธนาคารต่าง ๆ ได้รับภัยไซเบอร์ในรูปแบบต่าง ๆ เช่น พ.ศ. 2559 ธนาคารกลางแห่งหนึ่งในอาเซียนถูกยักยอกเงิน สถาบันการเงินไทย 2 แห่ง ถูกลักข้อมูลของลูกค้าบางส่วน และสรุปว่าปัจจัยจากไซเบอร์เป็นภัยร้ายแรง 1 ใน 5 ความเสี่ยงที่สำคัญระดับโลก

Phohom (2021) ได้สรุปข้อมูลว่า ไซเบอร์ หมายถึงถึง เทคโนโลยีทางไซเบอร์ในการค้นหาข้อมูล (Search engine) เช่น Google Yahoo เทคโนโลยีไซเบอร์ในรูปแบบพื้นที่ทางสังคม เช่น Facebook, X, Instagram, Line, Youtube, ระบบประชุมทางไกล (VDO Conference)

Rupkumdee et al. (2022) วิจัยพบว่า การประทุษวาจา (Hate Speech) การกลั่นแกล้งออนไลน์ (Cyberbullying) และแนวคิดหัวรุนแรง (Radicalization) บนสื่อออนไลน์ในประเทศไทย ส่วนใหญ่เป็นการเผยแพร่ภาพลามกอนาจาร การใช้ข้อความและภาพที่ไม่เหมาะสม เพราะสื่อออนไลน์ต่าง ๆ สามารถเข้าถึงได้ง่าย ขาดจิตสำนึกของกลุ่มบุคคลที่มุ่งผลประโยชน์ในเชิงพาณิชย์ โดยพบในแพลตฟอร์ม เช่น Facebook, X (Twitter), TikTok,

Instagram, YouTube และเว็บเพจต่าง ๆ ซึ่งส่งผลเสียต่อบุคคล สังคม วัฒนธรรม และประเทศชาติ

Matanboon (2022) วิจัยพบว่า เมื่อมีเวลาว่าง นักเรียนในจังหวัด เชียงรายจะเล่นอินเทอร์เน็ต ร้อยละ 27.8 โดยที่สามารถใช้โทรศัพท์หรือเครื่อง คอมพิวเตอร์โดยอิสระ ร้อยละ 93.7 โดยใช้เวลานั้นละ 4-6 ชั่วโมง อีกทั้งพบว่า นักเรียนวัยนี้เริ่มได้รับผลกระทบทางลบจากการเล่นเกมคอมพิวเตอร์และ อินเทอร์เน็ต หรืออาจเรียกว่า การได้รับผลกระทบทางลบจากไซเบอร์ โดยเคย ถูกนิทาผ่านระบบและนักเรียนให้ความเห็นว่าที่เกิดการกลั่นแกล้งกันในโลก คอมพิวเตอร์และอินเทอร์เน็ตหรือไซเบอร์ เพราะไม่ทราบว่าเป็นความผิด ร้อยละ 32.4

การจัดการกับภัยคุกคามทางไซเบอร์ของประเทศไทย

ประเทศไทยตระหนักถึงภัยคุกคามจากไซเบอร์ หรือมีต้นเหตุมาจาก ไซเบอร์ มีวิธีการต่าง ๆ (Phohom, 2021) ดังนี้

1. แผนยุทธศาสตร์ชาติ พ.ศ. 2561-2580 ออกแบบดำเนินการด้าน ความมั่นคงทางไซเบอร์แห่งชาติ โดยที่ปี พ.ศ. 2560-2564 รัฐบาลไทย ออกนโยบายฉบับแรกเกี่ยวกับการรับมือภัยคุกคามทางไซเบอร์ พ.ศ. 2562 ออก พ.ร.บ. การรักษาความมั่นคงปลอดภัยทางไซเบอร์
2. การจัดการกับภัยที่เกิดจากไซเบอร์ของหน่วยงานพลเมือง และให้ สำนักงานสภาความมั่นคงแห่งชาติ (สปช.) ช่วยรับผิดชอบภัยที่เกิดจากไซเบอร์
3. การจัดการกับภัยที่เกิดจากไซเบอร์ของหน่วยทหารกองทัพ โดยมี การจัดตั้งศูนย์ไซเบอร์กองทัพบก เป็นต้น



4. ภาครัฐออกกฎหมายอื่น ๆ ที่เกี่ยวกับข้อมูลส่วนบุคคลเกี่ยวกับการนำเข้าข้อมูลภาพเข้าระบบและเผยแพร่ หรือใช้คอมพิวเตอร์ และอินเทอร์เน็ตไปในการส่งข่าวเผยแพร่

นอกจากนี้ทุกองค์กรจะมีมาตรการแตกต่างกันออกไป เช่น ให้ความรู้ได้แก่ รายการข่าวก่อนแชร์ ของช่องทีวี อสมท. เป็นต้น (Thai News Agency, 2024) ที่ให้ความรู้ข่าวอะไรเป็นข่าวจริงที่แชร์ได้ อะไรเป็นข่าวปลอมไม่ควรแชร์

บทวิจารณ์

แม้้นประกาศต่าง ๆ จะมีมาตรการทางกฎหมายเพื่อคุ้มครองผู้ถูกระทำ และบทลงโทษผู้กระทำความผิด แต่การให้ความรู้และการแจ้งเตือนภัยจากไซเบอร์ที่แพร่ระบาดไปทั่วทั้งในประเทศที่มีเทคโนโลยีขั้นสูง แต่ประชาชนยังพบภัยจากไซเบอร์ ตัวอย่างเช่น ประเทศอังกฤษ ในปี พ.ศ. 2566 พบว่า มีภัยจากไซเบอร์ที่หลอกลวงให้หลงรักแล้วรีดทรัพย์ พบมาถึงร้อยละ 22 ภัยจากไซเบอร์ทั้งหมดทำความสูญเสียเหตุการณ์ละ 375,154 บาท (ThaiCERT, 2023) และสำหรับประเทศไทย จากการสำรวจของ NIDA Poll (2023) เรื่องภัยไซเบอร์ ระหว่างวันที่ 27 ตุลาคม 2566 ถึงวันที่ 3 พฤศจิกายน 2566 พบว่า ประชาชนมีความกังวลว่าจะถูกหลอกโดยแก๊งค์คอลเซ็นเตอร์ พบว่า ร้อยละ 54.20 จากกรณีที่ยกตัวอย่างในประเทศไทยที่มีเทคโนโลยีสูง ประชาชนยังถูกหลอก ได้รับภัยจากไซเบอร์และประเทศไทยประชาชนยังมีความกลัวที่จะพบแก๊งค์คอลเซ็นเตอร์



ภาครัฐอาจจะแสดงให้เห็นว่ามาตรการทางกฎหมาย มาตรการให้ความรู้ในสถานศึกษา ในรายการที่ถ่ายทอดต่าง ๆ ยังไม่สามารถที่จะหยุดภัยจากไซเบอร์ได้ ดังนั้น จึงควรจะมีมาตรการอื่น ๆ เข้ามาช่วยในการลดภัยคุกคามจากไซเบอร์ ถ้าเปรียบมาตรการทางกฎหมาย เป็นมาตรการแข็ง มาตรการอ่อนได้แก่ การสร้างความตระหนักรู้ ดังนั้น อาจถึงเวลาที่จะต้องให้มาตรการอ่อนเพิ่มขึ้น เช่น มาตรการทางวัฒนธรรม โดยกลุ่มแรกที่จะควรจะทำมาตรการทางวัฒนธรรมมาใช้ได้แก่ กลุ่มนักศึกษา ด้วยในแต่ละวัน นักศึกษามีเวลาอยู่กับไซเบอร์นานมากกว่ากลุ่มอื่น ๆ

โดยวางมาตรการทางวัฒนธรรมการตระหนักรู้ทันภัยไซเบอร์ไว้ ดังนี้

1. นักศึกษาระดับปริญญาตรี ซึ่งถือเป็นส่วนสำคัญในการสร้างวัฒนธรรมทางไซเบอร์เชิงบวก ทั้งนี้จะต้องมีการสร้างจิตสำนึกในการใช้งานการนำสื่อสังคมออนไลน์ไปใช้ในทางที่ถูกต้อง ไม่ก่อให้เกิดปัญหาหรือภัยคุกคามทางไซเบอร์

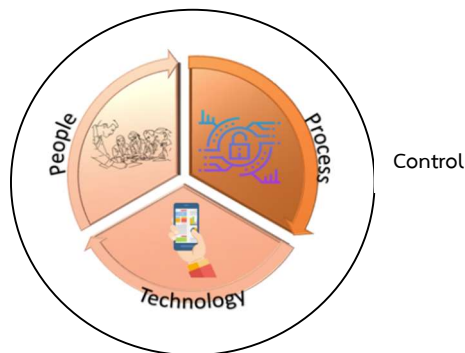
2. เทคโนโลยีและอุปกรณ์ ซึ่งเป็นปัจจัยที่นำมาใช้งาน ถือเป็นช่องทางในการติดต่อสื่อสารระหว่างผู้ส่งสารและผู้รับสาร การนำเทคโนโลยีหรืออุปกรณ์มาใช้หากนำมาใช้ในทางที่ผิดก็ทำให้เกิดปัญหาต่อสังคม ดังนั้น จะต้องการสร้างวัฒนธรรมไซเบอร์เชิงบวกจึงต้องเน้นถึงการนำเทคโนโลยีหรืออุปกรณ์มาใช้ไม่ให้เกิดปัญหา และการใช้เทคโนโลยีในการป้องกันภัยคุกคามทางไซเบอร์ได้

3. กระบวนการ หรือขั้นตอนการดำเนินกิจกรรม ทั้งนี้ มหาวิทยาลัยถือเป็นส่วนหนึ่งที่สำคัญในการสร้างกระบวนการวัฒนธรรมไซเบอร์เชิงบวกได้เป็น



อย่างดีในการสร้างจิตสำนึกให้กับนักศึกษาที่จะไม่ก่อให้เกิดปัญหาต่อสังคมหรือบุคคลอื่น ทั้งนี้ กระบวนการที่สำคัญในการสร้างวัฒนธรรมไซเบอร์เชิงบวกจะเป็นส่วนที่จะช่วยป้องกันและแก้ไขปัญหาเมื่อเกิดภัยคุกคามทางไซเบอร์ ซึ่งกระบวนการที่กล่าวถึงนี้ได้แก่ การสร้างความตระหนักรู้ เพื่อให้เกิดความรู้เท่าทันถึงภัยที่จะเกิดขึ้นเมื่อมีการนำอุปกรณ์มาใช้งาน และสามารถรับมือเพื่อแก้ไขสถานการณ์เมื่อเกิดเหตุได้ทัน่วงที ซึ่งกระบวนการนี้จะรวมถึงการฝึกอบรมให้กับบุคลากร นักศึกษาทุกคน

4. การควบคุม ตระหนักว่าหากกระทำสิ่งที่ไม่ถูกต้องจะมีผลกระทบต่อผู้อื่นและตนเอง



ภาพที่ 1 ห่วงโซ่ความสัมพันธ์

จากภาพแสดงถึงห่วงโซ่ความสัมพันธ์ที่มีทั้งสามส่วน คือ People ได้แก่ นักศึกษา หรือบุคลากรทางการศึกษา เทคโนโลยี ได้แก่ อุปกรณ์ที่นำมาใช้ในการสื่อสาร และกระบวนการ ได้แก่ กิจกรรมที่ก่อให้เกิดการเชื่อมโยงการ

ติดต่อสื่อสารผ่านทางโซเชียล ถือเป็นส่วนสำคัญในการสร้างวัฒนธรรมโซเชียลเชิงบวก และการควบคุมด้วยความรู้สึกว่าผู้อื่นเดือดร้อนและตนเองเดือดร้อนด้วยทำผิดกฎหมาย

สรุป

คำว่า “โซเชียล” หมายถึง การดำเนินการที่ใช้คอมพิวเตอร์ และระบบอินเทอร์เน็ต ดังนั้น สื่อออนไลน์ต่าง ๆ หรือเทคโนโลยีทางการสื่อสารต่าง ๆ เป็นส่วนหนึ่งของโซเชียล โซเชียลแพร่กระจายไปได้เร็วทั่วโลก ไปยังกลุ่มของประชาชน มีสาเหตุมาจาก โซเชียลเป็นนวัตกรรมที่เข้าถึงง่าย ใช้งานง่าย เมื่อใช้กันอย่างแพร่หลายจำนวนมาก ถูกพัฒนารูปแบบวิธีการใช้ จนมีค่าบริการต่ำ บางประเภทไม่เสียค่าบริการ เมื่อคนโกงหรือมิจฉาชีพนำโซเชียลมาเป็นเครื่องมือกลั่นแกล้งผู้อื่น จึงได้รับความเสียหายมาก และรวดเร็ว มาตรการทางกฎหมายไม่สามารถเอาผิด และติดตามกลุ่มผู้ใช้โซเชียลไปกลั่นแกล้งผู้อื่นได้ทั้งหมด และไม่สามารถหยุดความคิดกลั่นแกล้งได้

บทความนี้ จึงขอเสนอมาตรการทางวัฒนธรรมที่ดีงาม คิดและปฏิบัติเชิงบวก เห็นใจเพื่อนมนุษย์ เมื่อได้รับความเดือดร้อน โดยเน้นที่กลุ่มนักศึกษาด้วยเป็นผู้ที่อยู่กับโซเชียลในแต่ละวันมากกว่าอาชีพอื่น อีกทั้งเป็นวัยที่ก้าวสู่วัยทำงานที่ต้องรับผิดชอบต่อกับงานและบุคคลอื่น ๆ จำนวนมากต่อไปในอนาคต ภายใต้ความหมายของวัฒนธรรม คือ สิ่งที่จะทำความเจริญงอกงามให้แก่หมู่คณะ รวมหมายถึง วิถีชีวิตของหมู่คณะที่แสดงออกทางพฤติกรรม ภาษา และกิจกรรมทางสังคม ทั้งนี้ ได้นำเสนอวัฒนธรรมการใช้และการรับข้อความ ภาพ



เสียง จากไซเบอร์ไวในสวนบทวิจารณ์ ทั้งนี้ สรุปได้ว่า หากสร้างวัฒนธรรมการใช้และการรับรู้ถึงภัยคุกคามทางไซเบอร์ จะเกิดประโยชน์ ดังนี้

1. เพื่อส่งเสริมให้นักศึกษามีวัฒนธรรมไซเบอร์เชิงบวก
2. เพื่อให้ทราบถึงวิธีการนำสื่อโซเชียลไปใช้ในเชิงสร้างสรรค์
เกิดประโยชน์ต่อสังคม
3. เพื่อป้องกัน และลดปัญหาที่เกิดจากการใช้สื่อโซเชียลในทางที่ทำให้เกิดภัยคุกคาม และเป็นปัญหาต่อสังคม

โดยที่วัฒนธรรมเชิงบวกที่นักศึกษาระดับปริญญาตรีควรที่จะมีในตนเอง ได้แก่

1. ดำเนินการภายใต้สิทธิที่ตนเองมี
2. เทคโนโลยีที่ใช้จะใช้ภายใต้ความรู้จริงและเป็นประโยชน์ต่อตนเองและผู้อื่น
3. กระบวนการการใช้ไซเบอร์ทุกขั้นตอนต้องเข้าใจอย่างแท้จริง
4. การกระทำเกี่ยวกับไซเบอร์ทุกครั้งต้องพิจารณาว่าผลการกระทำตนเองจะต้องไม่เดือดร้อนและต้องไม่ผิดกฎหมาย

ข้อเสนอแนะเชิงนโยบาย

สถาบันการศึกษาควรมีนโยบายในการเพิ่มหลักสูตรการสร้างความรู้ตระหนักรู้ และวัฒนธรรมไซเบอร์เชิงบวก เพื่อป้องกัน ลดปัญหาจากการใช้งานสื่อโซเชียลในทางที่ทำให้เกิดภัยคุกคาม และเป็นปัญหาต่อสังคม รวมถึงนักศึกษาสามารถเผยแพร่ความรู้ให้กับประชาชนทั่วไปได้ และออกนโยบาย



นำกรณีศึกษาที่ใช้ไซเบอร์ทางลบแล้วตนเองและสังคมเดือดร้อนอย่างไร และผิดกฎหมายอย่างไรบ้าง ให้เกิดการตระหนักรู้

ข้อเสนอแนะการนำไปใช้

อาจารย์ผู้สอนแนะนำหลักของการสร้างวัฒนธรรมเชิงบวก 4 ข้อ แก่ลูกศิษย์ ด้วยเพราะจากนั้นจะแพร่กระจายไปกลุ่มอื่น ๆ ตามแนวคิด การแพร่กระจาย ซึ่งจะต้องเริ่มต้นสิ่งดีและมีการช่วยกันขับเคลื่อน

เอกสารอ้างอิง

Bank of Thailand. (2023) Top 3 Cyber threats that Thai people have been deceived the most. Retrieved from <https://shorturl.asia/luolh>

Chainwong, P., Skulphan, S., & Thapinta, D. (2020). Being Cyberbullied and Suicide Risk among Youths. *The Journal of Psychiatric Nursing and Mental Health*, 34(3), 133-151.

Cyber Security Maintenance ACT, B.E. 2019. (2019, 27 May). *Thai Government Gazette*, pp. 20-51.

Digital Economy Promotion Agency. (2019). *Digital Economy Promotion Agency action plan*. Retrieved from <https://www.depa.or.th/storage/app/media/Action%20Plan-depa-62.pdf>



Everett, M. Roger. (1995). *Diffusion of Innovations*. 4th ed. New York : Free Press.

Faculty of Science and Technology Dhonburi Rajabhat University.

(2019). Learning in the 21 century social media. Retrieved from <https://sci.dru.ac.th/dlr/files3/Media%20Online.pdf>

Kongboonma, T. (2019). The rule of law and the law on cybersecurity. Retrieved from https://www.constitutionalcourt.or.th/occ_web/ewt_dl_link.php?nid=11141

Longdo Dict. (2008). *Meaning of Cyber*. Retrieved from <https://dict.longdo.com/search/CYBER>

Matanboon, W. (2022). Violent Behavior in Media Usage among Children and Youth in Chiang Rai Province. *Thai Media Foun Journal*, 1(3), 1-31.

Matrakool, A., & lamviriyakul, I. (2018). *Cyber threats are one of the five major global risks, the financial sector is the main target of attacks*. Retrieved from <https://shorturl.asia/Q6eH4>

National Statistical Office Thailand. (2023). *Household Information and Communication Technology Use Survey 2023 (Q3)*. Bangkok: National Statistical Office Thailand.

- NIDA Poll. (2023). Cyber Threats. Retrieved from
<https://nidapoll.nida.ac.th/data/survey/uploads/FILE-1699009763644.pdf>
- NT Cyfence. (2022). *10 Cyber Threat Prevention Guidelines For small and medium-sized businesses*. Retrieved from
<https://www.cyfence.com/article/10-ways-to-prevent-cyber-threats-for-small-and-medium-businesses/>
- Office of the National Anti-Corruption Commission. (2021). *Anti-Corruption in Digital Disruption*. Retrieved from
<https://multi.dopa.go.th/acoc/assets/modules/news/uploads/0dec3410214c02cec7b616b91b1ee9a4615c192f1f9b76195411401018429554.pdf>
- Office of the Royal Society. (2020). *Cyberculture*. Retrieved from
<https://www.facebook.com/RatchabanditThai/photos/a.3083612691696805/3480081552049915/?type=3>
- Phohom, K. (2021). Thailand's Cyber Security Dynamics. *Journal of Security Perspectives*, 1(7), 45-54.
- Rogers, E. (2003). *Diffusion of Innovations*, New York, Free Press.
- Rupkumdee, V., Dokchaba, P., Imsiri, P., Andre, V., Sarvela, O., Boonying, V., & Lertputtarak, S. (2023). Guidelines for developing good practices and ethical standards for



presenting content on online media related to Hate Speech, Cyberbullying and Radicalization of the Thai Media Fund. *Thai Media Found Journal*, 2(4), 24-57.

Sangsuriyong, R. (2021). Transition to Cybersociety in Eastern Economic Corridor. *Academic Journal of Humanities and Social Sciences Burapha University*, 29(3), 241-269.

Sunyawiwat, S. (2007). *Sociological theory: content and basic utilitarianism*. Bangkok: Phimluk.

Tawekanachot, R. (2022). *Construction of cyber bully scale for undergraduate students*. M.Ed. Independent Study in Educational Research and Evaluation-(Plan B) Naresuan University.

Thai News Agency. (2024). *Sure and Share*. Retrieved from <https://tna.mcot.net/category/sureandshare>

ThaiCERT. (2023). *Statistics Report on Financial Results for the Year 2021-2023*. Retrieved from <https://shorturl.asia/Z3HK2>

Thairath. (2024). Collect and bounce the gun scolding. Lari shot dead 1 hurt 2 claimed revenge through social media. Retrieved from <https://www.thairath.co.th/news/crime/2760271>

The National Broadcasting and Telecommunication Commission. (2022). Studies to develop mechanisms or measures to

prevent bullying Intimidation and harassment of women
Children & Youth The campaign channel is conducted
through various multimedia media. Bangkok: Office of the
National Broadcasting and Telecommunications
Commission.

Thumronglaohapun, S., Kummaraka, U., Traisathit, P., Kardkasem,
R., Maneeton, B., Manojai, N., Chaijaruwanich, J., Limpiti
S., & Srikummoon, P. (2022). Impacts and proper
responses of cyberbullying in youth. *Thai Media Found
Journal*, 1(3), 1-22.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3
and a research agenda on interventions. *Decision
Science*, 39(2), 273-312.

Wikipedia. (2020). Cyberspace. Retrieved from
<https://shorturl.asia/o1E8e>

