ใบความรู้ที่ ๑ เรื่อง ภัยใกล้ตัว บนสังคมและสื่อออนไลน์
หน่วยการเรียนรู้ที่ ๓ เรื่อง สุขภาพดี มีทักษะชีวิต รู้ป้องกันภัย
แผนการจัดการเรียนรู้ที่ ๓ เรื่อง ภัยใกล้ตัว
รายวิชา สุขศึกษา รหัสวิชา พ ๒๒๑๐๓ ภาคเรียนที่ ๒ ชั้นมัธยมศึกษาปีที่ ๒

ภัยจากโลกออนไลน์ ถือเป็นเรื่องที่ไม่ควรมองข้าม เพราะนำมาซึ่งผลเสียทั้งด้านร่างกาย จิตใจ อีกทั้งนำไปสู่การล่อลวงต่อชีวิตและทรัพย์สิน

ความมั่นคงปลอดภัยทางไซเบอร์ หรือ Cyber Security คือ เทคโนโลยี กระบวนการและวิธีปฏิบัติที่ถูกออกแบบมาเพื่อปกป้องเครือข่าย อุปกรณ์ โปรแกรม และข้อมูลจากการโจมตีความเสียหายหรือการเข้าถึงจากบุคคลที่ ๓ โดยไม่ได้รับอนุญาต

ภัยคุกคามใกล้ตัว บนสังคมออนไลน์ที่พบส่วนใหญ่

๑. การถูกแฮกข้อมูล เพื่อลักลอบขโมยข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน หมายเลขบัตรเครดิต เลขบัญชีธนาคาร และรหัสสำคัญอื่นๆ ที่ใช้ทำธุรกรรม โดยอาจนำข้อมูลเหล่านี้ไปขายต่อหรือไปใช้ในทางที่เสียหาย

๒. ภัยที่มาจากการเชื่อมอินเทอร์เน็ตผ่านมือถือ ซึ่งทำแฮกเกอร์จะมีวิธีการหลอกลวงเพื่อดักจับข้อมูลหลายรูปแบบ เช่น ออกแบบหน้าเว็บไซต์ปลอมให้มีลักษณะคล้ายคลึงกับของจริง เพื่อให้ผู้ใช่งานเข้าใจผิด และหลงกรอกข้อมูลส่วนตัวเข้าสู่ระบบ จากนั้นก็จะส่งข้อมูลนี้ไปยัง เสิร์ฟเวอร์ (server) ของมิจฉาชีพในทันที โดยทันที **การโจมตีแบบนี้เรียกว่า ฟิชชิ่ง (phishing)** มักจะมาในรูปแบบการแนบลิงค์ไปกับอีเมล หรือลิงค์เชิญชวนต่างๆ ให้กดสนใจและกดลิงค์เข้าไปดู

๓. ภัยการโหลดแอปพลิเคชันต่างๆ มาใช้งานบนมือถืออย่างไม่ระมัดระวัง อาจทำให้เสี่ยงต่อการถูกโจมตีจากสปายแวร์และแรนซัมแวร์ ที่เป็นอันตรายต่อข้อมูลมือถือได้

๔. การเชื่อมต่ออินเทอร์เน็ตผ่านเครือข่ายไร้สาย หรือ WiFi โดยไม่ได้เข้ารหัสความปลอดภัย มีโอกาสถูกดักจับข้อมูลได้ง่าย สาเหตุ มักเกิดจากการเชื่อมต่อ WiFi สาธารณะ เช่น wifi ในร้านกาแฟ ร้านอาหารหรือในห้างสรรพสินค้า

ข้อมูลเพิ่มเติมและแนวทางการป้องกันตนเองจากภัยคุกคามบนสังคมออนไลน์

๑. การระรานทางไซเบอร์ (Cyber Bully) หมายถึง การกลั่นแกล้ง การให้ร้าย การด่าว่า การข่มเหง การรังแกผู้อื่น หรือ แสดงความคิดเห็น (Comment) หรือ เผยแพร่หรือส่งต่อข้อมูล (Share) ที่ทำให้ผู้อื่นเสียหาย ทางสื่อสังคมออนไลน์ อาจมีความผิดฐานหมิ่นประมาทโดยการโฆษณา ตามประมวลกฎหมายอาญา มาตรา ๓๒๘ มีอัตราโทษจำคุกไม่เกินสองปี หรือปรับไม่เกินสองแสนบาท ดังนั้นควรมีสติก่อนจะโพสต์ แสดงความคิดเห็น หรือ ส่งต่อข้อมูลในสื่อสังคมออนไลน์

๒. การถูกเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ (ถูกแฮก)

สาเหตุ

๑. เกิดจากการใช้รหัสที่คาดเดาได้ง่าย เช่น หมายเลขโทรศัพท์มือถือ วันเดือนปีเกิด เป็นต้น

๒. กดลิงก์ Phishing ที่สร้างลิงก์มาหลอกให้คลิก เช่น หลอกจะให้รางวัล บัตรกำนัล แจกเงิน แจกภาพ/คลิปลามกอนาจาร, ใบ้หวย เลขเด็ด, ข่าวซุบซิบดารา,หลอกว่าบัญชีธนาคารมีปัญหา เป็นต้น เมื่อเข้าไปในลิงก์ที่กดแล้ว คนร้ายจะให้กรอก Username Password หรือแม้กระทั่งมีการหลอกเอารหัสใช้ครั้งเดียว(OTP) โดยคนร้ายจะโทรศัพท์หรือแชทมาขอรหัสโดยอ้างว่าเป็นเจ้าหน้าที่ Call center หรือปลอมเป็นเพื่อนเรา

การป้องกันการถูกแฮก

๑. ต้องตั้งรหัสคาดเดาได้ยาก

๒. ไม่กดลิงก์แปลกๆ ที่ไม่มีที่มาที่ไปหรือไม่น่าเชื่อถือ

๓. ไม่บอกรหัส OTP แก่ผู้อื่น, ตั้งค่า รหัสยืนยันตัวตนแบบ ๒ ชั้น (๒ Factor Authentication) ในทุกสื่อสังคมออนไลน์ เป็นต้น

๓. การฉ้อโกงออนไลน์ในรูปแบบต่างๆ เช่น การหลอกซื้อของออนไลน์ในลักษณะซื้อของไม่ได้ของ หรือซื้อของแล้วได้ของไม่เป็นไปตามรูปแบบที่สั่ง (ไม่ตรงปก), หลอกให้ลงทุนโดยอ้างว่าได้ผลตอบแทนสูงในระยะเวลาสั้นๆ เป็นต้น

การป้องกันฉ้อโกงออนไลน์ สามารถทำได้ด้วยคาถา ๓ อย่า ดังนี้

๑. **อย่าเชื่อ** โดยนำชื่อนามสกุล หมายเลขบัญชีธนาคาร ชื่อร้านค้า ฯลฯ ไปหาข้อมูลใน google ว่าเคยมีประวัติการฉ้อโกงหรือไม่

๒. **อย่าโลภ** ไม่ควรเห็นแก่ผลประโยชน์ที่มิจฉาชีพมาอ้างเพื่อชักชวนลงทุนหรือสินค้าราคาถูกมากเกินจริง

๓. **อย่าละเลย** ข้อมูลข่าวสาร โดยเฉพาะข่าวเกี่ยวกับอาชญากรรมไซเบอร์ เพื่อจะรู้เท่าทันโจรไซเบอร์

๔. หลอกรักออนไลน์ (Romance Scam)

กรณีตัวอย่าง

๑. สร้างโปรไฟล์เป็นชาวต่างชาติ ฐานะดีมาจีบ สุดท้ายหลอกให้โอนเงินไปให้โดยอ้างเหตุต่างๆ

๒. หลอกรักลวงลงทุน (Hybrid Scam) โดยสร้างโปรไฟล์เป็นหนุ่มสาวหมวยตี๋ชาวเอเชีย มาจีบ สุดท้ายหลอกให้ลงทุนค่าเงินสกุลดิจิทัลในแอปพลิเคชันปลอมโดยคนร้ายจะส่งลิงก์มาให้

การป้องกันการหลอกรักออนไลน์และหลอกรักลวงลงทุน คือ เมื่อมีชาวต่างชาติขอเป็นเพื่อนแล้วมีการพูดคุย ในลักษณะจีบเป็นแฟน อาจตรวจสอบได้โดยขอนัดเจอตัวจริง หรือร้องขอให้เปิดกล้องวิดีโอคอล ให้เห็นหน้าเพื่อให้มั่นใจว่าเป็นบุคคลคนเดียวกับรูปในโปรไฟล์จริงๆ (หน้าตรงปก) ซึ่งส่วนใหญ่ คนร้ายจะไม่ยอมวิดีโอคอลโดยอ้างเหตุขัดข้องต่างๆ ให้สันนิษฐานไว้ก่อนว่าเป็นมิจฉาชีพ และไม่ควรโอนเงินให้ทุกกรณีที่มี การกล่าวอ้าง หรือลงทุนในแอปพลิเคชันที่มิจฉาชีพส่งลิงก์มาให้

๕. แก๊งแอปพลิเคชันเงินกู้ มีการระบาดมากโดยอาศัยปัญหาทางเศรษฐกิจของประชาชนในช่วงโควิด-๑๙ ตัวอย่างเช่น

กรณีที่ ๑ เข้ามาชักชวนให้ประชาชนกู้เงินผ่านแอปพลิเคชัน จากนั้นจะหลอกให้โอนเงินค่าธรรมเนียมก่อนกู้ เมื่อเหยื่อโอนเงินแล้วจะบล็อค

กรณีที่ ๒ ให้กู้เงินจริงแต่จะขูดรีดดอกเบี้ยเกินอัตราที่กฎหมายกำหนด เมื่อไม่ชำระหนี้ตามกำหนด จะมีการโทรศัพท์ขู่ ต่อว่าด้วยถ้อยคำหยาบคาย ดูหมิ่นเหยียดหยามผู้กู้ นอกจากนั้นจะมีการส่งข้อความหรือโทรศัพท์หาเพื่อนผู้กู้ในลักษณะประจานผู้กู้ หรือหลอกลวงให้เพื่อนผู้กู้มาชำระหนี้แทนโดยอ้างว่าเพื่อนผู้กู้เป็นผู้ค้ำประกัน จึงควรหลีกเลี่ยงการกู้เงินผ่านแอปพลิเคชันเงินกู้ทุกกรณี

๖. ข่าวปลอม (Fake News) เกิดขึ้นเมื่อมีบุคคลไม่หวังดีพยายามส่งข่าวปลอมเข้ามาในสื่อสังคมออนไลน์ **มีจุดประสงค์** เช่น สร้างความขัดแย้ง สร้างความเกลียดชัง สร้างความสับสน สร้างความตื่นตระหนกให้กับประชาชน เป็นต้น ดังนั้น จึงควรตรวจสอบข้อมูลว่าเป็นเรื่องจริงก่อนจะเชื่อและส่งต่อ เพราะอาจตกเป็นเครื่องมือของบุคคลหรือกลุ่มบุคคลที่ไม่หวังดี

สามารถตรวจสอบข้อมูล จากศูนย์ต่อต้านข่าวปลอมประเทศไทย www.antifakenewscenter.com หรือหน่วยงานราชการที่เกี่ยวข้อง หรือ สำนักข่าวที่น่าเชื่อถือ เป็นต้น ทั้งนี้หากไม่อยากตกเป็นเหยื่อของอาชญากรรมในทุกรูปแบบที่ว่ามา จึงควรระมัดระวังและศึกษาข้อมูลและตรวจสอบรายละเอียดในโลกออนไลน์ทุกครั้งก่อนปฏิบัติการใดๆ ไป

หากพบเห็นการกระทำผิดกฎหมายดังกล่าว กรุณาแจ้งเบาะแสไปยังสายด่วน ๑๙๑ และสายด่วนสำนักงานตำรวจแห่งชาติ ๑๕๙๙ ได้ตลอด ๒๔ ชั่วโมง

๗. การล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต

สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime: UNODC) ได้นำเสนอวิธีการล่อลวงเด็กเพื่อนำไปล่วงละเมิดทางเพศผ่านทางอินเทอร์เน็ต คือ มีการตระเตรียมเด็กสำหรับการล่วงละเมิดทางเพศออนไลน์ (Online Grooming)

การตระเตรียมเด็กสำหรับการล่วงละเมิดทางเพศออนไลน์ หมายถึง การกระทำของผู้ใหญ่ซึ่งเป็นการสร้างปฏิสัมพันธ์และความไว้เนื้อเชื่อใจกับเด็กผ่านการสื่อสารทางอินเทอร์เน็ต โดยมีวัตถุประสงค์เพื่อการล่วงละเมิดทางเพศ ไม่ว่าจะในรูปแบบออนไลน์หรือออฟไลน์ก็ตาม โดยผู้กระทำความผิดอาจเริ่มจากการคัดเลือกเหยื่อซึ่งเป็นเด็กตามสื่อสังคมออนไลน์ ซึ่งบุคคลเหล่านี้ถือเป็นกลุ่มเปราะบาง ง่ายต่อการเข้าถึง และเป็นผู้ที่มีโอกาสจะหลงเชื่อบุคคลได้ง่าย เช่น บัญชีสื่อสังคมออนไลน์ของเด็กที่อนุญาตให้ทุกคนสามารถเข้าถึงข้อมูลส่วนตัวและความเคลื่อนไหวได้ (Visible to the Public) เป็นต้น

จากนั้นก็จะทำการติดต่อไปยังเด็กเพื่อพูดคุยสร้างปฏิสัมพันธ์และความไว้เนื้อเชื่อใจในห้องสนทนา (Chatroom) จนเกิดการล่วงละเมิดทางเพศในที่สุดพฤติกรรมการก่อเหตุมักเริ่มจากการศึกษาข้อมูลส่วนตัวของเด็กเพื่อเริ่มต้นการสนทนาด้วยการนำเข้าสู่เรื่องที่เด็กสนใจ เช่น งานอดิเรก เกมที่ชื่นชอบ ดาราที่ชื่นชอบ หรือสถานภาพทางเศรษฐกิจ เป็นต้น หลังจากนั้นจะเป็นการใช้ถ้อยคำหรือข้อความเพื่อสานความสัมพันธ์ในเชิงฉันท์ชู้สาวจนนำไปสู่การร้องขอให้มีกิจกรรมทางเพศ เช่น การส่งภาพหรือวิดีโออันมีลักษณะลามกอนาจาร เป็นต้น ซึ่งในเวลาต่อมาอาชญากรก็จะข่มขู่และควบคุมให้เด็กซึ่งตกเป็นผู้เสียหายส่งสื่ออิเล็กทรอนิกส์ในลักษณะดังกล่าวเพิ่มขึ้นอย่างต่อเนื่อง

วิธีกันตนเอง

๑. ไม่รับแอดคนแปลกหน้าเป็นเพื่อนในโซเชียลมีเดีย

๒. ไม่เปิดเผยข้อมูลส่วนตัวหรือตำแหน่งที่อยู่ในสื่อออนไลน์

๓.

๔. ไม่โพสน์แบบโป๊เปลือยแม้รูปนั้นจะเป็นรูปเด็กเล็กก็ตาม

ที่มาภาพ : คณะปราบปรามการล่วงละเมิดทางเพศ

ทักษะที่สำคัญอีกประการหนึ่ง ในการรอดพ้นภัยใกล้ตัว บนสังคมและสื่อออนไลน์ คือ

การรู้เท่าทันสื่อ คือ ความสามารถป้องกันตนเองจากการถูกจูงใจจากเนื้อหาของสื่อการสามารถวิเคราะห์เนื้อหาของสื่ออย่างมีวิจารณญาณ เพื่อให้สามารถควบคุมการตีความเนื้อหาของสื่อที่มีปฏิสัมพันธ์คือ การที่เราไม่หลงเชื่อเนื้อหาที่ได้อ่าน ได้ยิน ได้ฟัง แต่สามารถคิด วิเคราะห์ แยกแยะ และรู้จักตั้งคำถาม

องค์ประกอบของการรู้เท่าทันสื่อ

๑. การเปิดรับสื่อ การเปิดรับการเข้าใจการวิเคราะห์สื่อ คือ การรู้เท่าทันการเปิดรับสื่อของประสาทสัมผัส หู ตา จมูก ลิ้น สัมผัสของเรา ซึ่งเมื่อเปิดรับแล้วสมองจะสั่งการให้คิดและปรุงแต่งให้เกิดอารมณ์ต่าง ๆ ตามมา การรู้เท่าทันสื่อในชั้นของการรับรู้อารมณ์ตนเองจึงเป็นสิ่งสำคัญที่ต้องแยกความคิดและอารมณ์ออกจากกัน และความคิดจะทำให้เรารับรู้ความจริงว่า "อะไรเป็นสิ่งที่สื่อสร้างขึ้น" เป็นต้น

๒. การวิเคราะห์สื่อ คือ การแยกแยะองค์ประกอบในการนำเสนอของสื่อว่ามีวัตถุประสงค์อะไร

๓. การเข้าใจสื่อ การตีความสื่อหลังจากเปิดรับสื่อไปแล้ว เพื่อทำความเข้าใจในสิ่งที่สื่อนำเสนอ ซึ่งผู้รับสารแต่ละคนเข้าใจสื่อได้ไม่เหมือนกันตีความไปคนละแบบ ขึ้นอยู่กับประสบการณ์ พื้นฐานการศึกษาคุณสมบัติในการเรียนรู้ ตลอดจนการรับรู้ข้อมูลของแต่ละบุคคลที่ไม่เท่ากันมาก่อน

๔. การประเมินค่า หลังการวิเคราะห์และทำความเข้าใจสื่อแล้ว เราควรประเมินค่าสิ่งที่สื่อนำสนอว่ามีคุณภาพและคุณค่ามากน้อยเพียงใดไม่ว่าจะเป็นด้านเนื้อหา วิธีนำเสนอเทคนิคที่ใช้ เป็นต้น

๕. การใช้สื่อให้เกิดประโยชน์ แม้เราจะสามารถวิเคราะห์ เข้าใจ และประเมินค่าสื่อได้ แต่เราไม่สามารถออกไปจากโลกของสื่อได้ ดังนั้นเราจึงจำเป็นต้องปฏิบัติดังนี้ คือ

- นำสิ่งที่เราวิเคราะห์ไปใช้ประโยชน์
- เลือกรับสื่อเป็น
- สามารถส่งสารต่อได้
- มีปฏิกิริยาตอบกลับสื่อได้
- นำสิ่งที่วิเคราะห์ไปใช้ประโยชน์
- เลือกรับสื่อเป็น
- สามารถส่งสารต่อได้
- มีปฏิกิริยาตอบกลับสื่อได้

องค์ประกอบนี้เป็นพื้นฐานอันดีของการเป็นผู้ผลิตสื่อที่ดี สำหรับผู้ที่สมารถคิดวิเคราะห์ เข้าใจธรรมชาติของสื่อได้เป็นอย่างดีแล้วเราอาจเป็นผู้ผลิตสื่อเอง โดยก่อให้เกิดสื่อดีๆ มีประโยชน์เพื่อสังคม โดยการวางแผนการจัดการสื่ออย่างเหมาะสมและเลือกข้อมูลเพื่อคิดเขียน พูดให้สอดคล้องกับวัตถุประสงค์ที่ต้องการภายใต้การผลิตสื่อที่มีความรับผิดชอบต่อสังคมองค์ประกอบนี้เป็นพื้นฐานอันดีของการเป็นผู้ผลิตสื่อที่ดี

แหล่งอ้างอิง

สำนักงาน กสทช. (๒๕๖๔). มารู้ทันโลกออนไลน์ กับ "Cyber Security ตอน ระวังภัยร้ายบนโลกไซเบอร์". จาก https://youtu.be/Zm๙sz-oTYYM

คณะทำงานปราบปรามการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต. (๒๕๖๒). สื่อออนไลน์ทำให้เด็กถูกล่วงละเมิดทางเพศได้อย่างไร. จาก https://youtu.be/ce๗al๕e๖Jjw

ศิริวัฒน์ ดีพอ. (๒๕๖๔). ระวังภัยออนไลน์ ๖ ประเภท. จาก https://www.pptvhd๓๖.com/news/อาชญากรรม/๑๕๔๒๖๔

อัศว์ณุต แสงทองดี. (๒๕๖๔). รูปแบบการล่วงละเมิดทางเพศต่อเด็กทางอินเทอร์เน็ต. วารสารวิชาการอาชญาวิทยาและนิติวิทยาศาสตร์. (ออนไลน์)

วาริน โพพันธุ์. (๒๕๖๓). การรู้เท่าทันสื่อ. จาก https://kru-it.com/computing-science-p๓/media-literacy/