

ใบความรู้

เรื่อง การใช้เทคโนโลยีสารสนเทศอย่างปลอดภัย

เทคโนโลยี (Technology) ตามพจนานุกรมราชบัณฑิตยสถาน คือ วิทยาการที่นำเอาความรู้ทางวิทยาศาสตร์มาใช้ให้เกิดประโยชน์ในทางปฏิบัติ เช่น อุตสาหกรรม เป็นต้น

สารสนเทศ (Information) ตามพจนานุกรมราชบัณฑิตยสถาน คือการแสดงหรือชี้แจงข่าวสารข้อมูลต่าง ๆ เทคโนโลยีสารสนเทศ (IT : Information Technology) หมายถึง การนำวิทยาการที่ก้าวหน้าทางด้านคอมพิวเตอร์และ การสื่อสารมาสร้างมูลค่าเพิ่มให้กับสารสนเทศ ทำให้สารสนเทศ มีประโยชน์และใช้งาน ได้กว้างขวางมากขึ้น

ในปัจจุบันเทคโนโลยีมีบทบาทในชีวิตประจำวัน ของเราทุก คน เราจึงจำเป็นต้องมีความรู้ความเข้าใจ ในการใช้เทคโนโลยีให้ถูกต้องปลอดภัย ทั้งกับตนเองและผู้อื่น

ภัยคุกคามจากการใช้เทคโนโลยีสารสนเทศและการป้องกัน

ปัจจุบันอินเทอร์เน็ตเข้ามามีบทบาทในการใช้ชีวิตประจำวัน ไม่ว่าจะเป็นด้านการศึกษา การดำรงชีวิต การสื่อสาร การศึกษา และอื่น ๆ อีกมากมาย เมื่อมีความสะดวกสบายมากเท่าใด ความปลอดภัยของข้อมูลที่เราจะนำเข้าไปในระบบยิ่งเป็นสิ่งที่สำคัญ การเผยแพร่ การนำเข้าไปข้อมูลต่าง ๆ ก็เช่นกัน ดังนั้นจึงมีความ จำเป็นที่จะต้องเรียนรู้และทำความเข้าใจ

1. วิธีคุกคามทางเทคโนโลยี

1.1 การคุกคามโดยใช้หลักจิตวิทยา เป็นการคุกคามที่ใช้การหลอกลวงเพื่อให้ได้ข้อมูลที่ต้องการโดยไม่ต้องใช้ความชำนาญด้านไอที เช่น การใช้กลวิธีการต่าง ๆ เพื่อให้ได้รหัสผ่านหรือส่งข้อมูลที่สำคัญให้ โดย หลอกว่า จะได้รับรางวัลแต่ต้องทำตามเงื่อนไขที่กำหนด ซึ่งสิ่งที่เกิดขึ้นอาจป้องกันได้ยากเพราะเกิดจาก ความเชื่อใจ แต่ป้องกันได้โดยให้นักเรียนระมัดระวังในการให้ข้อมูลส่วนตัวกับบุคคลอื่น

1.2 การคุกคามด้วยเนื้อหาที่ไม่เหมาะสม ข้อมูลและเนื้อหาที่มีอยู่ในแหล่งต่าง ๆ บนอินเทอร์เน็ตมีเป็นจำนวนมากเพราะสามารถสร้างและเผยแพร่ได้ง่าย ทำให้ข้อมูลอาจไม่ได้รับการตรวจสอบความถูกต้อง และความเหมาะสม ดังนั้นข้อมูลบางส่วนอาจก่อให้เกิดปัญหากับนักเรียนได้

แหล่งข้อมูลที่มีเนื้อหาไม่เหมาะสม ได้แก่ แหล่งข้อมูลที่เกี่ยวข้องกับความรุนแรง การยุยงให้เกิดความแตกแยก วนเวียนในสังคม การพนัน สื่อลามกอนาจาร เนื้อหาที่เป็นการหมิ่นประมาท และการกระทำที่ เกี่ยวข้องกับสิ่งที่มีผิดต่อกฎหมายและจริยธรรม

1.3 การคุกคามโดยใช้โปรแกรม เป็นการคุกคามโดยใช้โปรแกรมเป็นเครื่องมือสำหรับก่อปัญหาด้านไอ ที โปรแกรมดังกล่าวเรียกว่า มัลแวร์ (malicious software: malware) ซึ่งมีหลายประเภท เช่น ไวรัส คอมพิวเตอร์

(Computer Virus), เวิร์ม (Worm), ม้าโทรจัน (Trojan Horse Virus) ส�파ยแวร์ (Spyware) โปรแกรมโฆษณา (Advertising Supported Software: Adware) และ โปรแกรมเรียกค่าไถ่ (Ransomware)

สามารถศึกษาข้อมูลการคุกคามโดยใช้โปรแกรมเพิ่มเติมได้ที่วีดิทัศน์ “ภัยคุกคามทางคอมพิวเตอร์” (URL: <https://www.youtube.com/watch?v=nkRjJMRSWCw>)

2. การป้องกันภัยคุกคาม

การป้องกันภัยคุกคามด้านเทคโนโลยี เราสามารถทำได้โดย การตรวจสอบและยืนยันตัวตนของตัวผู้ใช้งานก่อนเริ่มใช้งาน ซึ่งมีด้วยกัน 3 รูปแบบคือ

2.1 ตรวจสอบจากสิ่งที่ผู้ใช้รู้ เช่น ชื่อผู้ใช้และรหัสผ่าน (Username & password) วิธีนี้ได้รับความ นิยมสูงสุด

2.2 ตรวจสอบจากสิ่งที่ผู้ใช้มี เป็นการตรวจสอบตัวตนจากอุปกรณ์ที่ผู้ใช้งานต้องมี เช่น บัตร สมาร์ทการ์ด

2.3 ตรวจสอบจากสิ่งที่เป็นส่วนหนึ่งของผู้ใช้ เป็นการตรวจสอบข้อมูลชีวมาตร เช่น ลายนิ้วมือ ม่านตา ใบหน้า เสียง

3. การตั้งรหัสผ่าน

รหัสผ่านถือเป็นสิ่งสำคัญในยุคของเทคโนโลยี การเข้าใช้งานระบบต่าง ๆ บนอินเทอร์เน็ต จำเป็นต้องมี ชื่อผู้ใช้และรหัสผ่านเพื่อเข้าใช้งาน การตั้งรหัสผ่าน จำเป็นต้องมีความปลอดภัยกับเจ้าของ เพื่อป้องกัน การรั่วไหลของข้อมูล หรือ การใช้แอคเคาน์ ไปในทางที่ผิด ดังนั้นในการตั้งรหัสผ่านให้มีความปลอดภัย สามารถปฏิบัติได้ดังนี้

- บัญชีรายชื่อผู้ใช้แต่ละระบบ ควรใช้รหัสผ่านที่แตกต่างกัน โดยเฉพาะบัญชีที่ใช้เข้าถึงข้อมูลที่มีความสำคัญ เช่น รหัสผ่านที่ใช้ในการเข้าถึง ข้อมูลที่มีความสำคัญ เช่น รหัสผ่านของบัตรเอทีเอ็ม หลีกเลี่ยงการใช้รหัสผ่านต่างกัน

- หลีกเลี่ยงการใช้รหัสผ่านโดยใช้วัน เดือน ปีเกิด ชื่อผู้ใช้ ชื่อจังหวัด ชื่อตัวละคร ชื่อสิ่งของต่าง ๆ ที่เกี่ยวข้อง หรือคำที่มีอยู่ในพจนานุกรม

- รหัสผ่านที่มีความยาว 10 ตัวอักษรนั้นเดายากกว่ารหัสผ่าน 8 ตัวอักษรถึง 4 พันเท่า ถ้าเดารหัสผ่าน 8 ตัวอักษรใช้เวลา 1 วัน เดารหัสผ่าน 10 ตัวอักษรก็ต้องใช้เวลา 4000 วัน เว็บไซต์ในทุกวันนี้มักจะ ต้องการรหัสผ่านความยาว 8 ตัวอักษรเป็นขั้นต่ำอยู่แล้ว แต่ถ้าต้องการความปลอดภัยจริง ๆ 10 ตัวอักษรจะดีกว่า

- ผสมผสานทั้งตัวเลข เครื่องหมาย ตัวอักษรใหญ่ และตัวอักษรเล็ก เมื่อเราใช้ตัวอักษรใหญ่ เล็ก ตัวเลข และเครื่องหมายต่าง ๆ ลงในรหัสผ่าน โอกาสที่จะเดารหัสผ่านถูกจะมีแค่ 1 ในหลายแสนล้าน - ไม่บันทึกหรือจดรหัสผ่านแบบอัตโนมัติบนโปรแกรม Browser โดยเฉพาะหากเครื่องคอมพิวเตอร์นั้นเป็น เครื่องที่ใช้ร่วมกับผู้อื่น

- หลีกเลี่ยงการบันทึกหรือส่งผ่านลงในกระดาษ รวมทั้งอุปกรณ์อิเล็กทรอนิกส์ด้วย หากจำเป็นต้องบันทึก ก็ควรจัดเก็บไว้ในที่ที่ปลอดภัย

- ไม่บอกหรือส่งผ่านของตนเองกับผู้อื่น ไม่ว่ากรณีใด ๆ

- หมั่นเปลี่ยนเป็นประจำ อาจกระทำทุก 3 เดือน

- ออกจากระบบทุกครั้งที่ใช้บริการต่าง ๆ บนอินเทอร์เน็ต

การใช้เทคโนโลยีสารสนเทศอย่างมีความรับผิดชอบ

1. แนวทางการปฏิบัติเมื่อพบเนื้อหาที่ไม่เหมาะสม

- ปฏิเสธการรับข้อมูล ทำได้โดยไม่เปิดดู ไม่บันทึกเก็บไว้ และไม่กดไลค์ (Like)

- ไม่ส่งต่อ ไม่แชร์ ไม่เผยแพร่ เพราะนอกจากจะทำให้ผู้อื่นเดือดร้อนกับข้อมูลที่ไม่เป็นความจริงแล้ว ยังอาจจะผิด พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งมีโทษทั้งจำทั้งปรับ

- แจ้งครู หรือ ผู้ปกครอง

- แจ้งผู้เกี่ยวข้องที่ดูแลเว็บไซต์นั้น เช่น Facebook YouTube เพื่อให้เจ้าของเว็บไซต์ ลบเนื้อหา หรือ ตัดสิทธิ์ (block) หรือจำกัดสิทธิ์การใช้งาน

- แจ้งเจ้าหน้าที่รัฐหรือตำรวจ เพื่อดำเนินการตามกฎหมาย

2. ผลกระทบการเผยแพร่ข้อมูลที่ไม่เหมาะสม

2.1 ด้านจิตใจ

- ต่อผู้เผยแพร่ รู้สึกผิดกับการกระทำของตนเอง หรือรู้สึกเสียใจเมื่อผู้อื่นมีพฤติกรรมเลียนแบบการกระทำที่ไม่เหมาะสม

- ต่อผู้อื่น เกิดความเสียใจ ทำให้เกิดความรู้สึกอับอาย ไม่ปลอดภัย กลัว รู้สึกไม่มั่นคง มีบาดแผลทางจิตใจ ได้รับความเกลียดชัง สูญเสียการยอมรับจากผู้อื่น

2.2 ด้านสังคม

- ต่อผู้เผยแพร่ ถูกสังคมลงโทษ ได้รับการประณาม หรือเกลียดชังจากสังคม

- ต่อผู้อื่น ได้ผลกระทบด้านการใช้ชีวิตประจำวัน ครอบครัวเดือดร้อน ถูกประณามจากสังคม 2.3 ด้านกฎหมาย

- ต่อผู้เผยแพร่ ได้รับโทษ เนื่องจากข้อมูลเหล่านั้นอาจผิดระเบียบ กฎเกณฑ์ หรือ กฎหมาย ทำให้เสียเวลา และเสียค่าใช้จ่ายจากการดำเนินคดีตามกฎหมาย

2.4 การงานและธุรกิจ

- ต่อผู้อื่น อาจถูกให้ออกจากงานเพราะบริษัทเกิดความเข้าใจผิดจากข้อมูลที่ได้รับ เสียผลประโยชน์ ทางธุรกิจ เช่น ผู้แสวงหาผลประโยชน์ หรือคู่แข่งทางธุรกิจ อาจสร้างข่าวลวง โฆษณาชวนเชื่อ เพื่อสร้างความเสียหายให้กับธุรกิจคู่แข่ง

3. แนวทางการพิจารณาเนื้อหา ก่อนการเผยแพร่ข้อมูล

ก่อนที่จะเผยแพร่ข้อมูลลงในอินเทอร์เน็ตต้องพิจารณาสิ่งต่อไปนี้

3.1 ความเป็นส่วนตัว (privacy) ต้องทราบว่าข้อมูลนั้นเกี่ยวข้องกับใครหรือองค์กรใดบ้าง สามารถเปิดเผยต่อผู้อื่นได้หรือไม่

3.2 ความถูกต้อง (accuracy) ข้อมูลที่ใช้ต้องมีความถูกต้อง มีความน่าเชื่อถือ

3.3 ทรัพย์สินหรือความเป็นเจ้าของ ต้องรู้ว่าใครเป็นเจ้าของข้อมูล มีความสำคัญหรือมูลค่ามากน้อยเพียงใด

3.4 การเข้าถึง เป็นการกำหนดหรือระบุให้บุคคลหรือองค์กรใดที่มีสิทธิ์ในการเข้าถึง

4. มารยาทในการติดต่อสื่อสาร

4.1 มารยาทในการใช้อีเมล

- ใช้ภาษาสุภาพ ชัดเจน ตรงประเด็น เหมาะสมกับกาลเทศะหรือผู้ที่สื่อสารด้วย - ใช้อักษรตัวหนาเฉพาะข้อความที่ต้องการเน้นเท่านั้น

- ระบุหัวเรื่อง ชื่อผู้ที่สื่อสาร และระบุตัวตนของผู้ส่งให้ชัดเจน

- ระบุชื่อ หรือตำแหน่งของผู้ที่จะสื่อสารให้ถูกต้องเหมาะสม

- ข้อความในอีเมลไม่ควรมีข้อความแสดงถึงเจตนาในทางเสื่อมเสีย ไม่ใช่ข้อความที่กำกวม แสดงถึง การตำหนิ ถูกใส่ร้ายผู้อื่นให้ได้รับความเสียหาย

- ไม่ลึกลับส่งอีเมลโดยการปลอมแปลงชื่อผู้ส่งจนทำให้ผู้รับเข้าใจผิด

- ไม่ส่งต่ออีเมลลูกโซ่

- ไม่ส่งอีเมลขายสินค้า โฆษณา หรือข้อความรบกวนผู้อื่น

4.2 มารยาทในการใช้แชทและเครือข่ายสังคมออนไลน์

เครือข่ายสังคมออนไลน์ หรือ โซเชียลมีเดีย (Social Media) คือได้ว่าเป็นเครือข่ายสังคมออนไลน์ที่เชื่อมโยงคนหลายคนเข้าไว้ด้วยกันผ่านอินเทอร์เน็ต มีอิทธิพลต่อการดำเนินชีวิตของผู้คนเกือบทุก ๆ ด้าน ซึ่งเครือข่ายสังคมออนไลน์มีทั้งข้อดี ข้อเสีย ซึ่งผู้ใช้ในการเผยแพร่ข้อมูลส่วนตัวออกไป และทุกคนสามารถ เข้าถึงข้อมูลของใครก็ได้ ข้อมูลของที่เผยแพร่ออกไปจะมีความเสี่ยงที่จะโดนแอบอ้างหรือขโมยความเป็น ส่วนตัว หรือขโมยความเป็นตัวตนบนโลกออนไลน์และอาจเป็นอันตรายต่อตัวเรามากกว่าที่คิด ฉะนั้นเรา ต้องดูแลตัวเอง ป้องกันไม่ให้เราเกิดภัยเนื่องจากการแชร์ข้อมูลส่วนตัวบนโลกออนไลน์ ซึ่งมีรายละเอียด ดังนี้

- ไม่ควรตั้งโปรไฟล์เป็นสาธารณะ
- ไม่ให้ข้อมูลส่วนตัวมากเกินไป ไม่ว่าจะเป็นวันเดือนปีเกิด เบอร์โทรศัพท์ ที่อยู่ บัตรประจำตัว ประชาชน หรือบัตรเครดิตลงในโซเชียล ไม่ว่าจะเป็นอยู่ในรูปแบบข้อความ หรือรูปภาพ คิดให้ รอบคอบก่อนโพสต์ข้อมูลใด ๆ
- คัดกรองคนที่ขอเป็นเพื่อน เราควรศึกษาดี ๆ ต้องเช็คให้ดีกว่าก่อน ว่าคนนั้นเป็นใครเป็นเพื่อนของ เพื่อนจริงหรือเปล่า และแอดเราเป็นเพื่อนเพื่อวัตถุประสงค์ใด ถ้าไม่เป็นเพื่อนของเพื่อนจริงเราก็ ไม่ขอรับเพื่อนดีกว่า เพราะว่าเขาอาจมีวัตถุประสงค์อื่นในการที่เข้ามาเป็นเพื่อนกับเรา
- การเช็คอินในสถานที่ต่าง ๆ เป็นการบอกว่าตอนนี้คุณอยู่ที่ไหน บางครั้งการโพสรูปของเราว่าไป เที่ยวอยู่จะกลับบ้านวันนั้นวันนี้ถ้าเป็นการแชร์กันระหว่างเพื่อนก็ไม่เป็นไร แต่ว่าถ้าคนอื่นที่ไม่ได้ เป็นเพื่อนเราจริง ๆ ก็ อาจจะเข้ามาประสงค์ร้ายได้
- ใช้ความระมัดระวังในการคลิกลิงก์ต่าง ๆ ที่มากับการแชร์หรือข้อความ หลีกเลี่ยงลิงก์แปลกปลอม หรือมาจากคนที่ไม่รู้จัก ซึ่งโลกออนไลน์เดี๋ยวนี้ไม่ค่อยมีการกลั่นกรองข่าวสารที่ดีพอ เพราะ อาจจะไปเจอลิงก์ข่าวปลอม หรืออาจเป็นลิงก์ที่นำไปสู่ไวรัสหรือช่องทางขโมยข้อมูลของเหล่าแฮกเกอร์ได้
- ไม่ให้เบาะแสของรหัสผ่านกับคนอื่น หลายคนอาจจะแชร์ว่าหมาของเราชื่อว่าอะไร เราชอบกีฬาประเภทไหน แต่สิ่งเหล่านี้ อาจจะเป็นคำถามเมื่อเราลืมรหัสผ่าน เข้าอีเมลต่าง ๆ ซึ่งถ้ามีผู้ไม่ ประสงค์ดีเข้ามาคอยติดตามก็อาจจะรู้ว่าเราชอบอะไรมีสัตว์เลี้ยงตัวไหน ชอบกีฬาชนิดใดอะไร อะไร และเขาก็สามารถเอาไปใช้เพื่อที่จะได้เอารหัสผ่านมาได้
- ไม่โพสต์รูปที่ไม่เหมาะสม เช่น โพสต์รูปตัวเองเมา หรือ โพสต์รูปตัวเองกำลังถือปืน หรือโพสต์รูป ที่สื่อไปทางอนาจาร หรืออื่น ๆ เพราะสิ่งเหล่านี้ อาจเป็นผลกระทบกับภาพลักษณ์ของตัวเอง - เปิดใช้งาน Do Not Track เพื่อป้องกันการติดตามและการเก็บข้อมูลของผู้ให้บริการ ซึ่งอาจรวม ไปถึงผู้ไม่หวังดีที่ลักลอบเข้ามาขโมยข้อมูลด้วย

- ใช้วิจารณญาณอย่างสูงในการรับข่าวสาร และอย่าปักใจเชื่อข้อมูลที่เผยแพร่เข้ามาในทันที รวมทั้ง การกล่าวอ้างถึงแหล่งที่มาของข้อมูลนั้น ๆ เพราะอาจมีการสวมรอย หรือสมอ้างจากผู้ไม่หวังดี เพื่อสร้างข่าว หรือสร้างความเสื่อมเสียต่อแหล่งที่มา นั้นได้

- ไม่โพสต์เรื่องดราม่าต่าง ๆ เป็นเรื่องเกี่ยวกับชีวิตส่วนตัว เช่น ว่าแฟนนอกใจ ทะเลาะกับเพื่อน ไม่พอใจเพื่อนร่วมงานอะไรต่าง ๆ การโพสต์แบบนี้จะเป็นการพาดพิงถึงบุคคลที่สาม อาจจะทำให้ เกิดเรื่องบานปลายได้

- ยุคนี้เป็นสังคมเสรี มีอิสระทางความคิดเห็น แม้ว่าทุกคนจะมีสิทธิ์ในการแสดงความคิดเห็น แต่ทุก คำพูด และการกระทำที่ไม่เหมาะสมก็สามารถเป็นเหตุในการฟ้องร้องได้ และศาลก็อาจจะรับฟัง คำร้องด้วย รวมถึงมี พ.ร.บ.ทางคอมพิวเตอร์ด้วย

- ไม่ใช่ข้อความที่เป็นชนวนก่อให้เกิดปัญหาระหว่างบุคคลและกลุ่ม

- หลีกเลี่ยงการใช้อารมณ์หรือความรู้สึกที่มากจนเกินไปทั้งในการอ่านหรือแสดงความคิดเห็น - ไม่สวมรอยหรือแอบอ้างโดยใช้ชื่อบุคคลอื่นในการแชท แสดงความคิดเห็น หรือทำให้ผู้อื่นได้รับความเสียหาย เพราะเป็นการกระทำที่ผิดกฎหมาย

- ไม่ใช่ถ้อยคำที่ยั่วยุหรือทำทนาย เพื่อแสดงความคิดเห็น หรือความคิดเห็นที่ขัดแย้งกับผู้อื่น

แหล่งอ้างอิง

ธงชัย แผลกไธสง (2561). ภัยคุกคามจากเทคโนโลยี. สืบค้นเมื่อวันที่ 20 พฤศจิกายน 2562, จาก <https://sites.google.com/a/sesao8.go.th/kruzam-computing-science/kar-chi-thekhnoloyi-xyang-plxdphay>

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี. เทคโนโลยี(วิทยาการคำนวณ) 1 . กรุงเทพฯ : ศูนย์หนังสือแห่งจุฬาลงกรณ์มหาวิทยาลัย. 2560.

สถาบันส่งเสริมการสอนวิทยาศาสตร์และเทคโนโลยี. เทคโนโลยี(วิทยาการคำนวณ) 2 . กรุงเทพฯ : ศูนย์หนังสือแห่งจุฬาลงกรณ์มหาวิทยาลัย. 2560.

สำนักงานราชบัณฑิตยสภา (2560). พจนานุกรม ฉบับราชบัณฑิตยสถาน พ.ศ. 2554. สืบค้นเมื่อวันที่ 20 พฤศจิกายน 2562, จาก <http://www.royin.go.th/dictionary/index.php>

สำนักงานกิจการยุติธรรม (2560). กฎหมายใหม่ 36.1 : 9 ข้อระวังภัย คนใช้โซเชียล. สืบค้นเมื่อวันที่ 22 พฤศจิกายน 2562, จาก <https://www.facebook.com/weareoja/photos/a.6644805936377161073741828.533062563446187/1362978923787876/?type=3&permPage=1>

A Time Design (2561). 15 ข้อควรระวัง! ในการใช้ SOCIAL MEDIA ให้ปลอดภัย รู้เท่าทัน ไม่ตกเป็นเหยื่อ. สืบค้นเมื่อวันที่ 22 พฤศจิกายน 2562, <http://www.atimedesign.com/webdesign/how-to-use-social-media-safety/>