

สรุปบทเรียนจากการพัฒนาความรู้

หลักสูตร

ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ
(Understanding and Using Digital Technology)

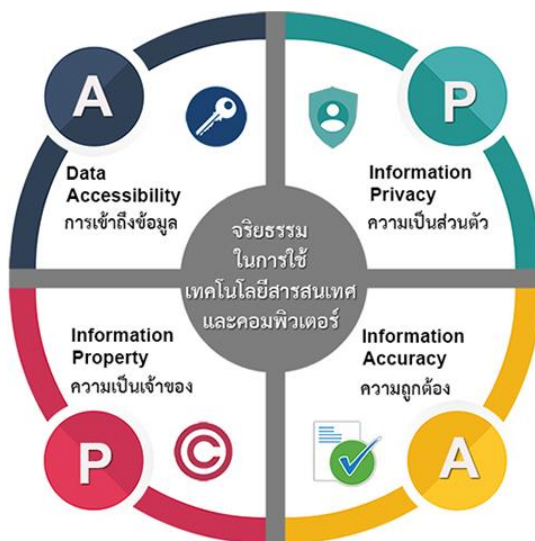
จัดทำโดย นายสทรรฐ์ เชาว์วิไล



ทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัล หรือ Digital literacy หมายถึง ทักษะในการนำเครื่องมืออุปกรณ์และเทคโนโลยีดิจิทัลที่มีอยู่ในปัจจุบัน เช่น คอมพิวเตอร์ โทรศัพท์ แท็บเล็ต โปรแกรมคอมพิวเตอร์ และสื่อออนไลน์ มาใช้ให้เกิดประโยชน์สูงสุด ในการสื่อสาร การปฏิบัติงาน และการทำงานร่วมกัน หรือใช้เพื่อพัฒนาระบบการทำงาน หรือระบบงาน หรือระบบงานในองค์กรให้มีความทันสมัยและมีประสิทธิภาพ

จริยธรรมในการใช้เทคโนโลยีสารสนเทศ

จริยธรรมในการใช้งานคอมพิวเตอร์และสารสนเทศจะกล่าวถึง 4 ประเด็น ในลักษณะตัวย่อว่า PAPA



1) ความเป็นส่วนตัว (Privacy) การควบคุมข้อมูลของตนเองในการเปิดเผยให้กับผู้อื่น เมื่อมีผู้คุกคาม เช่น เข้ามาอ่าน e-mail ติดตามผู้ใช้เพื่อทำการส่ง e-mail ขยายสินค้า ทำให้เกิดอีเมลขยะ (junk mail) ที่ผู้รับไม่ต้องการเรียกว่า สปแอม ซึ่งถือว่าการละเมิดความเป็นส่วนตัว

2) ความถูกต้อง (Accuracy) ความถูกต้องของข้อมูลมีผู้รับผิดชอบ ข้อมูลมีความทันสมัยอยู่เสมอ เช่น ถ้าลูกค้าป้อนข้อมูลเองต้องให้สิทธิในการเข้าไปตรวจสอบความถูกต้องด้วยตนเอง

3) ความเป็นเจ้าของ (Property) กรรมสิทธิ์ในการถือครอง โดยทรัพย์สินแบ่งเป็น 2 ประเภท คือ ทรัพย์สินที่จับต้องได้ เช่น คอมพิวเตอร์ รถยนต์ และทรัพย์สินที่จับต้องไม่ได้ เช่น ทรัพย์สินทางปัญญา

4) การเข้าถึงข้อมูล (Data accessibility) เพื่อการป้องกันการเข้าไปดำเนินการกับข้อมูลของผู้ใช้ที่ไม่มีส่วนเกี่ยวข้องและเป็นการรักษาความลับของข้อมูล

การเข้าถึงสื่อสารยุคดิจิทัล

สื่อดิจิทัล หมายถึง สื่อที่นำเอาข้อความ กราฟิก ภาพเคลื่อนไหว เสียง มาจัดรูปแบบ โดยอาศัยเทคโนโลยี และการสื่อสารมาประยุกต์ใช้ ทำให้ลดค่าใช้จ่ายและระยะเวลา สื่อดิจิทัลสามารถแบ่งออกเป็น 5 ประเภท คือ ภาพดิจิทัล เสียงดิจิทัล วิดีโอดิจิทัล ทิวทัศน์ดิจิทัล และอินเทอร์เน็ตดิจิทัล

การค้นหาข้อมูลในอินเทอร์เน็ตเสิร์ชเอนจิน (Search Engine) ซึ่งจะต้องกรอกคีย์เวิร์ด (Keyword) ข้อมูลที่ต้องการค้นหา ระบบจะแสดงผลลัพธ์ของคำที่เราค้นหา โดยมีเทคนิคการค้นหาดังนี้

- การไม่เอาคำที่ต้องการ ให้ใช้เครื่องหมายลบหน้าคำ
- การระบุค่าเป็นวลี ให้ใช้เครื่องหมายคำพูด
- การค้นหาโดยใช้คำหลายคำ ให้ใช้ OR เช่น “โลกร้อน” OR “เรือนกระจก”
- การค้นหาข้อความในเว็บนั้น ให้ใช้ site:url keyword
- การค้นหาเฉพาะประเภทไฟล์ ให้ใช้ filetype:PDF keyword
- ค้นหาคำที่ไม่รู้ในวลีนั้น ให้ใช้ *(ดอกจัน) เช่น A * History of Philosophy ได้ผลลัพธ์เป็น A Little History of Philosophy
- หาเว็บที่เกี่ยวข้อง ให้ใช้ related:url
- หาเฉพาะหัวข้อเรื่อง ให้ใช้ intitle:keyword
- ค้นหาโดยใช้ภาพ หากจาก <https://images.google.com> (ใช้ตรวจสอบหาต้นฉบับภาพได้)
- การแปลงหน่วย, แปลงค่าเงิน เช่น 100 USD to TH

ความเข้าใจและการสื่อสารยุคดิจิทัล

ทุกวันนี้ วิธีการสื่อสารของเรานั้นดูเหมือนจะไม่ใช่การโทรศัพท์หากันอีกต่อไป แต่กลายเป็นการส่งข้อความผ่านทางเครือข่ายสังคมออนไลน์ หรือที่เรียกว่า Social Network นั่นเอง ซึ่งแนวโน้มความนิยมใช้ Social Network ทำให้เห็นว่าสิ่งนี้จะกลายเป็นสื่อหลักในการสื่อสารอย่างแน่นอน เรียกว่าเป็น “ยุคของการแพร่หลายทางสังคมออนไลน์ (Social Ubiquity)”

Social Network มีข้อดีมากมาย โดยเฉพาะในการแสดงออกทางความคิด และกิจกรรมต่างๆ รวมทั้งการรับรู้ข้อมูลจากผู้อื่น ด้านธุรกิจอีคอมเมิร์ซก็เช่นกัน Social Network ทำให้ผู้ขายได้ประชาสัมพันธ์ได้ง่ายขึ้น ผู้ซื้อก็มีโอกาสเข้าถึงสินค้าได้ง่ายเช่นกัน แต่การที่ผู้ใช้งาน Social Network มีโอกาสเผยแพร่ข้อมูลได้ง่าย รวมทั้งทุกคนสามารถใช้งานได้ ก็ทำให้ข้อมูลใน Social Network อาจจะเป็นข้อมูลที่ไม่ถูกต้อง อีกทั้งมีโอกาที่จะสูญเสียความเป็นส่วนตัวไปได้ ซึ่งแน่นอนว่าคงไม่เสมอไปที่เราจะเจอกับปัญหาต่างๆ ใน Social Network แต่การรู้ทันปัญหาที่อาจเกิดขึ้นได้นั้น ก็เป็นการดีที่เราจะได้ป้องกันและระวังภัยต่างๆ ได้ ดังนี้

1. คิดให้รอบคอบก่อนโพสต์ข้อมูลใดๆ เพราะอย่าลืมว่าข้อมูลเหล่านี้จะเปิดเผยให้ทุกคนสามารถเข้าถึงได้ง่าย โดยเฉพาะอย่างยิ่งการโพสต์ข้อมูลที่สุ่มเสี่ยงก็อาจจะส่งผลร้ายต่อตัวเราเองก็เป็นได้
2. ใช้ความระมัดระวังในการคลิกลิงก์ต่างๆ ที่มาจากการแชร์หรือข้อความ หลีกเลี่ยงลิงก์แปลกปลอม หรือมาจากคนที่ไม่รู้จัก หรือแม้แต่เพื่อนซึ่งใช้ภาษาในการสื่อสารที่ดูแปลกไปจากปกติ เพราะอาจเป็นลิงก์ที่นำไปสู่ไวรัส หรือช่องทางขโมยข้อมูลของเหล่าแฮกเกอร์
3. พิมพ์ที่อยู่ URL ของเว็บไซต์โซเชียลเน็ตเวิร์กนั้นๆ โดยตรง โดยบนเบราว์เซอร์ให้หลีกเลี่ยงการเข้าเครือข่ายทางสังคมผ่านทางคลิกลิงก์จากผลแสดงการค้นหา หรือจากอีเมล เพราะอาจเป็น URL ปลอมที่นำเราไปยังเว็บไซต์ปลอม เพื่อหลอกเอาบัญชีผู้ใช้และ Password ได้ เช่น www.facebook.com อาจมี URL หลอกเป็น www.faebook.com เป็นต้น
4. คัดกรองคนที่ขอเป็นเพื่อน หรือขอเชื่อมโยงกับเครือข่ายสังคมออนไลน์ของเรา หลีกเลี่ยงการตอบรับคนที่ไม่รู้จักกันมาก่อน เพราะผู้ไม่หวังดีอาจแฝงมากับคนที่ขอเข้ามาเป็นเพื่อนเรา และหากพบคนที่เป็เพื่อนซึ่งเราไม่รู้จักและน่าสงสัยก็ควรลบออกไป

5. ตั้งค่าความเป็นส่วนตัว ผู้ให้บริการแต่ละรายจะกำหนดการตั้งค่าส่วนตัวไว้เพื่อไม่ให้ข้อมูล หรือสิ่งที่เราทำหลุดออกไปยังคนที่ไม่พึงประสงค์ ดังนั้น เราควรตั้งค่าให้เพื่อนเท่านั้นที่เห็นกิจกรรมของเรา และหลีกเลี่ยงการตั้งค่าสิ่งที่เราทำให้เป็นสาธารณะ หรือคนทั่วไปเห็นได้

6. ไม่แสดงข้อมูลส่วนตัวที่เป็นความลับ เช่น บัตรประจำตัวประชาชน บัตรเครดิตลงในโซเชียลเน็ตเวิร์ก ไม่ว่าจะอยู่ในรูปแบบข้อความ หรือรูปภาพ เพราะแฮกเกอร์และผู้ไม่หวังดีสามารถแฝงตัวมากับกลุ่มเพื่อนที่เราอนุญาตให้เข้าชมได้

7. เปิดใช้งาน Do Not Track เพื่อป้องกันการติดตามและการเก็บข้อมูลของผู้ให้บริการ ซึ่งอาจรวมไปถึงผู้ไม่หวังดีที่ลักลอบเข้ามาขโมยข้อมูลด้วย ซึ่งปัจจุบันมีเว็บเบราว์เซอร์ที่เปิดใช้งาน Do Not Track ได้แล้ว เช่น Internet Explorer 10

8. ใช้วิจารณญาณอย่างสูงในการรับข่าวสาร และอย่าปักใจเชื่อข้อมูลที่เผยแพร่เข้ามาในทันที รวมทั้งการกล่าวอ้างถึงแหล่งที่มาของข้อมูลนั้นๆ เพราะอาจมีการสวมรอย หรือสมอ้างจากผู้ไม่หวังดีเพื่อสร้างข่าว หรือสร้างความเสื่อมเสียต่อแหล่งที่มาได้

9. ดูแลและควบคุมการใช้งานของบุตรหลานอย่างใกล้ชิด สอนให้เด็กรู้จักวิเคราะห์ข้อมูล และรู้จักเล่นอย่างถูกวิธี เพราะความรู้ในโซเชียลเน็ตเวิร์กก็มีอยู่มากมาย และปัจจุบันครูอาจารย์ก็ทันสมัยจนแจ้งเรื่องต่างๆ แก่ลูกศิษย์ผ่านโซเชียลเน็ตเวิร์ก เช่น Facebook หรือ Twitter กันแล้ว นอกจากนี้ อาจหาเครื่องมือในการควบคุมการใช้งานของบุตรหลานได้ เช่น โปรแกรม Windows Live Family Safety ซึ่งเป็นโปรแกรมที่ไม่โครซอฟต์เปิดให้ใช้งานได้ฟรีๆ นอกจากจะใช้ควบคุมการเข้าถึงเว็บไซต์ที่มีเนื้อหาไม่เหมาะสมได้แล้ว ยังสามารถกำหนดช่วงเวลาในการใช้คอมพิวเตอร์ และป้องกันการใช้โปรแกรม หรือเล่นเกมที่ไม่เหมาะสมหรือไม่ได้รับอนุญาตได้อีกด้วย

10. ตระหนักว่ามันเป็นสังคมเสรี แม้ว่าทุกคนจะมีสิทธิในการแสดงความคิดเห็น แต่ทุกคำพูดและการกระทำที่ไม่เหมาะสมก็สามารถเป็นเหตุในการฟ้องร้องได้ และศาลก็อาจจะรับฟังคำร้องด้วย

การหลบหลีกภัย Social Network คงไม่ใช่การเลิกใช้งานไปเลย เพราะยังมีประโยชน์ดีๆ อีกมากมายในเครือข่ายสังคมออนไลน์นี้ แต่ถ้ารู้จักใช้อย่างระมัดระวังก็จะช่วยให้เราสามารถสนุกสนานกับสังคมออนไลน์อย่างมั่นใจมากขึ้น อย่างไรก็ตาม แนวทางปฏิบัติเหล่านี้ก็อาจมีขั้นตอนที่แตกต่างกันไปตามแต่ละ Social Network ที่เราสามารถศึกษาได้จากคำแนะนำบนเว็บไซต์เหล่านั้น

ความปลอดภัยยุคดิจิทัล

โลกดิจิทัลได้เปลี่ยนวิถีชีวิตของผู้คนในยุคปัจจุบันในหลายๆ ด้าน เช่น วิธีการติดต่อกับเพื่อนและคนรู้จัก การทำธุรกรรมทางการเงิน การซื้อขายสินค้า และการรับชมสันทนาการความบันเทิงต่างๆ แต่อย่างไรก็ตามโลกไซเบอร์ซึ่งรวมถึง อินเทอร์เน็ต เครือข่ายสังคมออนไลน์ โทรศัพท์มือถือ เกมออนไลน์ แอปพลิเคชัน และอื่นๆ ยังมีภัยคุกคามที่แฝงมากับความสะดวกสบายและความบันเทิงเหล่านี้ด้วย ดังนั้นเราจึงควรรู้จักป้องกันปกป้องตัวตน Digital บนโลกออนไลน์ของเรา ได้ดังนี้

1. ตั้งรหัสผ่านที่เดายาก ไม่ใช่ซ้ำ และหมั่นเปลี่ยนอยู่เสมอ

วิธีง่าย ๆ ที่เราสามารถทำได้คือ การตั้งรหัสผ่านที่คาดเดายากและหลากหลาย มีความยาวอย่างน้อย 12-14 ตัวอักษร ประกอบไปด้วย ตัวอักษรใหญ่ ตัวอักษรเล็ก ตัวเลข และไม่ควรรู้ซ้ำกับ Online Account อื่น ๆ รวมถึงคอยตรวจสอบค่าขอรีเซตรหัสผ่านในบัญชีด้วย และที่สำคัญควรเปลี่ยนรหัสผ่านเป็นประจำทุก 3- 6 เดือน เพื่อป้องกันกรณีที่มีการรั่วไหลของข้อมูลโดยที่เราไม่รู้ตัว

2. หมั่น Update ระบบปฏิบัติการบนอุปกรณ์

หมั่นตรวจสอบการ Update ระบบปฏิบัติการและการตั้งค่าเบราว์เซอร์อุปกรณ์ต่างให้ทันสมัยอยู่เสมอ เช่น โทรศัพท์มือถือ คอมพิวเตอร์ แล็ปท็อป ฯลฯ เพราะ แพทช์ทุกเวอร์ชันย่อมมีช่องโหว่ที่แฮกเกอร์สามารถเข้ามายังระบบได้ แต่เมื่อเราหมั่น Update แพทช์ ก็จะช่วยปิดช่องโหว่นั้น ๆ และ เพิ่มฟีเจอร์ใหม่ๆ ที่ช่วยให้มีความปลอดภัยระบบมากขึ้นหรือหากระบบปฏิบัติการผิดพลาดจนไม่สามารถใช้งานได้ เราจะได้แก้ไขอย่างทันท่วงที

3. หลีกเลี่ยงการใช้ Wi-Fi สาธารณะ

พยายามหลีกเลี่ยงการใช้ Wi-Fi สาธารณะ ทางที่ดีควรใช้อินเทอร์เน็ตเครือข่ายมือถือของตัวเองเพราะเราไม่สามารถรู้ได้ว่า เครือข่าย Wi-Fi สาธารณะปลอดภัยจริงหรือไม่ เป็น Wi-Fi ปลอมที่แฮกเกอร์สร้างเพื่อดักจับข้อมูลเหยื่อหรือเปล่า หากไม่มีทางเลือกควรใช้ VPN (Virtual Private Networks) ด้วย เพื่อให้แน่ใจว่ากิจกรรมออนไลน์ทั้งหมดจะปลอดภัยตั้งแต่ ฐานการออนไลน์ไปจนถึงข้อความส่วนตัว

4. อย่าแชร์ทุกอย่างที่คิด ก่อนแชร์ให้คิดก่อนเสมอ

ในโลก Social media มีอันตรายแอบแฝงอยู่แล้ว ยิ่งถ้าเราใช้งานโดยการแชร์ทุกอย่างที่เกี่ยวข้องกับเราลงบนโลกออนไลน์ เช่น แชร์ข้อมูลส่วนตัวทั้งหมดแบบสาธารณะ แชร์ Location ที่อยู่อาศัยของตัวเอง ฯลฯ อาจเป็นการแบ่งปันข้อมูลให้กับแฮกเกอร์ หรือ คนแปลกหน้าก็ได้ ทางที่ดีควรคิดก่อนแชร์เสมอ เพื่อความปลอดภัยของตัวเอง

5. จดบันทึกประวัติการใช้งานทางการเงิน

จดบันทึกการใช้งานเครดิตอยู่เสมอว่าเราได้ใช้ทำอะไร ที่ไหน เวลาเท่าไร และจดบันทึกการเปลี่ยนแปลงแม้จะเล็ก ๆ น้อย ๆ เพื่อป้องกันยอดเงินแปลกๆ ที่หักเงินในบัตรเครดิตเราแบบที่ไม่รู้ตัวและที่สำคัญไม่ควรผูกเลขบัตรเครดิต เลขบัญชีธนาคารลงในเว็บไซต์ช้อปปิ้งออนไลน์ หรือ เว็บไซต์ Social ต่าง ๆ เพราะหากโดนแฮกบัญชี สิ่งพวกนี้คือเป้าหมายแรกของแฮกเกอร์ในการขโมยข้อมูล

6. ตรวจสอบประวัติการใช้งานอินเทอร์เน็ตเสมอ

ตรวจสอบการใช้ซอฟต์แวร์เพื่อป้องกันการติดตามต่างๆ และป้องกันข้อมูลส่วนบุคคลบนโลก Social (ข้อมูลส่วนตัวที่คุณโพสต์ไว้บน Profile Digital ต่าง ๆ) ของเราเพื่อรักษาตัวเองให้ปลอดภัยจากการติดตามออนไลน์ที่ถูกคุกคามโดยโฆษณาออนไลน์ต่าง ๆ ที่ไม่เหมาะสม

7. ใช้ระบบรักษาความปลอดภัยในทุกอุปกรณ์ที่เชื่อมต่อออนไลน์

ถ้าคอมพิวเตอร์หรืออุปกรณ์ชิ้นนั้น สามารถออกสู่โลกอินเทอร์เน็ตได้ ต้องป้องกันมันด้วย เช่น ถ้าเป็น PC หรือ มือถือ ก็จะต้องมี Antivirus เพื่อป้องกันการโดนไวรัส หรือถ้าถ้าในอนาคตตู้เย็นส่งข้อมูลออกสู่โลกอินเทอร์เน็ตได้ ก็ควรจะต้องป้องกันมันด้วย เพราะทุกการเชื่อมต่อมีภัยแฝงเสมอ การเลือกระบบรักษาความปลอดภัยจึงเป็นเรื่องสำคัญ

แหล่งที่มา

หลักสูตร : ความเข้าใจและการใช้เทคโนโลยีดิจิทัลอย่างมีประสิทธิภาพ

บรรยายโดย : ผศ. ดร. โชติศักดิ์ ธรรมบุษดี สาขาวิชาเทคโนโลยีการจัดการระบบสารสนเทศ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล และคณะ

สถาบัน/หน่วยงาน/ระบบ : ระบบฝึกอบรมผ่านสื่ออิเล็กทรอนิกส์ ของสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล Thailand Digital Government Academy (TDGA)

รูปแบบหลักสูตร : e-Learning

ช่วงเวลาการฝึกอบรม : ส.ค. 2566