



คู่มือ การสร้าง ความตระหนักรู้ ในการใช้ชีวิตระบบที่ดี

ETDA DIGITAL CITIZEN PLUS



คู่มือ การสร้าง ความตระหนักรู้ ในการใช้ชีวิตระบบนิร์สุ่น

ETDA DIGITAL CITIZEN PLUS

สแกนเพื่อเข้าสู่
หลักสูตรออนไลน์



คู่มือ การสร้าง ความตระหนักรู้ ในการใช้อินเทอร์เน็ต

ETDA DIGITAL CITIZEN PLUS

พิมพ์ครั้งแรก กรกฎาคม 2567

ส่วนสิทธิ์โดย : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

Electronic Transactions Development Agency

ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

คู่มือการสร้างความตระหนักรู้ในการใช้อินเทอร์เน็ต ETDA DIGITAL CITIZEN PLUS.–

กรุงเทพฯ : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2567.

362 หน้า.

1. เทคโนโลยี – แสั่งคอมวิทยา. 2. อินเทอร์เน็ต – แสั่งคอม. I. ชื่อเรื่อง.

303.483

ISBN 978-616-7956-63-3

จัดพิมพ์โดย สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา (อาคารบี)

ชั้นที่ 6 เลขที่ 120 หมู่ที่ 3 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง

เขตหลักสี่ กรุงเทพมหานคร 10210

โทรศัพท์ : 02 123 1234 โทรสาร : 02 123 1200

พิมพ์ที่ บริษัท พีดับบลิว พรินติ้ง จำกัด



แนะนำการใช้คู่มือ



ยกระดับทักษะ

ความคาดการณ์ดิจิทัลก้าว 5 ด้าน

หน้า 1 - 45

ด้านที่ 1

อัตลักษณ์ดิจิทัล
Digital Identity



หน้า 47 - 117

ด้านที่ 2

การใช้เทคโนโลยีดิจิทัล
อย่างเหมาะสม
Digital Use



หน้า 119 - 167

ด้านที่ 3

การจัดการ
ความปลอดภัย
ในโลกดิจิทัล
Digital Security



หน้า 169 - 233

ด้านที่ 4

การสื่อสารดิจิทัล
Digital Communication



หน้า 235 - 337

ด้านที่ 5

การรู้เท่าทันดิจิทัล
Digital Literacy



สัญลักษณ์พิเศษที่ใช้ในคู่มือ

เพื่อช่วยในการเลือกเนื้อหา หรือระบุถึงความสำคัญ และความพิเศษของเนื้อหา คู่มือเล่มนี้จึงได้มีการทำเครื่องหมายด้วยสัญลักษณ์ไอคอนตามคุณสมบัติของข้อมูล ดังต่อไปนี้

REMEMBER

สัญลักษณ์นี้หมายถึง

ประเด็นหรือข้อมูลที่สำคัญ ควรจดจำให้ดี



TIP

สัญลักษณ์นี้หมายถึง

เคล็ดลับ คำแนะนำต่าง ๆ ที่มีประโยชน์
ควรนำไปปรับใช้



WARNING

สัญลักษณ์นี้หมายถึง

ป้ายเตือนภัย ที่ควรใส่ใจระมัดระวัง
ถึงผลกระทบ ความเสี่ยง
และอันตราย ที่อาจตามมา

EXAMPLE

สัญลักษณ์นี้หมายถึง

ประเด็นหรือข้อมูลที่ต้องการยกตัวอย่าง
เพื่อให้ผู้อ่านเข้าใจในเนื้อหามากยิ่งขึ้น



คำนำ



“ขอคำนำสำหรับคู่มือ EDC Plus
เล่นนี้แบบลื้น ๆ”

AI : “คุณมือเล่นนี้เป็นแหล่งความรู้และแนวทาง
สำหรับ “First Jobber” ในระดับพื้นฐาน เพื่อ
พัฒนาทักษะดิจิทัลทั้ง 5 ด้าน ตามหลักสูตร
ETDA Digital Citizen (EDC) ฉบับปรับปรุงใหม่
เพื่อให้พร้อมรับมือ กับ โลภการทำงานยุคดิจิทัล
เนื้อหาภายในครอบคลุมตั้งแต่ พื้นฐานการใช้งาน
เทคโนโลยีดิจิทัล การรู้เท่าทันสื่อ ไปจนถึงการใช้
ประโยชน์จากเทคโนโลยีดิจิทัล เพื่อการทำงาน
และพัฒนาตนเอง”



จากบทสนทนาริจิข้างต้น ที่เราขอให้ AI รายหนึ่งช่วยเขียนคำนำคู่มือเล่นนี้อกมา
ภายใน 3 วินาที เป็นหลักฐานเชิงประจักษ์ที่ชัดเจนว่า การใช้ชีวิตในยุคดิจิทัลปัจจุบัน
และอนาคต มุ่งมั่นที่จะทำให้เราสามารถท้าทายมากเพียงใด

อีกทั้งยังมีความท้าทายจากหลากหลายองค์ความรู้เกี่ยวกับเทคโนโลยีดิจิทัลที่ปัจจุบัน
กล่าวเป็น “Minimum Requirements” หรือความรู้จำเป็นขั้นพื้นฐานสำหรับคน
ทำงานและทุกคนที่เกี่ยวพันกับเทคโนโลยีดิจิทัล

คำนำ



- การรู้จักปกป้องดูแลตัวตนบนโลกดิจิทัล ไม่ให้เสื่อมเสีย และไม่ถูกสวมรอยขโมยตัวตน
- การรู้จัก “ใช้งาน” ไม่ใช่ “ถูกใช้งาน” โดยอุปกรณ์ดิจิทัล บริการดิจิทัล หรือสังคมดิจิทัล
- เราจะปักป้องทรัพย์สินและสิ่งมีค่าของเราและองค์กร ท่ามกลางการโจมตีทางไซเบอร์ ที่ลึกซึ้งได้อย่างไร
- “เจ็บใจ เจ็บปวด อย่างที่ไม่เคยรู้สึกมาก่อน เพราะโลกดิจิทัลหรือเปล่า ?” จะริง ๆ แล้ว เราควรจัดการและจำกัดการเปิดรับและส่งสารอย่างไร
- ในยุคที่เราต้องพึ่งพาข้อมูลมากขึ้น แต่ความเชื่อถือได้ กลับยิ่งลดลงอย่างลงตัว เราควรรับมืออย่างไร
- ที่สำคัญ เราต้องเตรียมตัวอย่างไร เมื่อยุคแห่ง AI มาถึงอย่างเต็มที่

ข่าวดี คือ เราสามารถรับมือสิ่งเหล่านี้ได้ ด้วยการมี “ทักษะความฉลาดทางดิจิทัล” หรือ DQ (Digital Intelligence Quotient) ซึ่งบรรจุอยู่ในคู่มือฉบับนี้ ครอบคลุม DQ สำคัญ 5 ด้าน

คุณไม่จำเป็นต้องอ่านเรียงกันตั้งแต่ต้นจนจบ ขอให้เริ่มต้นที่เรื่องที่ใกล้ตัวและสนใจที่สุด เพราะคู่มือเล่มนี้เป็นของคุณ คุณสามารถย้อนกลับมาอ่านเพิ่มเติมได้ทุกเมื่อ

ยิ่งไปกว่านั้น คุณสามารถใช้คู่มือเล่มนี้ ประกอบกับ หลักสูตรออนไลน์เรียนฟรี EDC Plus ซึ่งหยิบยกเนื้อหามาดำเนินสอนด้วยรูปแบบที่เข้าใจง่ายขึ้น ภายในเวลาไม่ถึง 3 ชั่วโมง พร้อมมอบวุฒิบัตรดิจิทัลเป็นหลักฐานแห่งการเรียนรู้และผ่านการทดสอบ

หากพร้อมแล้วที่จะยกระดับ “ทักษะความฉลาดทางดิจิทัล” ไปด้วยกัน ขอเชิญพลิกเข้าสู่เนื้อหา EDC Plus ในหน้าตัดไปได้ทันที

ด้วยความปรารถนาดี

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)

คำนิยม

EDC TRAINER รุ่น 1



คุณวชิรา พงศ์พยัคฆ์

EDC ให้ความรู้ในการรับมือกับโลกดิจิทัลที่กำลังเป็นส่วนหนึ่งของชีวิต ได้ทั้งประโยชน์และปรับเรื่องราวไปใช้ได้ เมماกับคนทุกวัย โดยเฉพาะกลุ่มสูงวัย ทั้งต่อยอดไปเป็นกิจกรรมสนุก ๆ ให้โลกดิจิทัลเป็นเรื่องที่ไม่น่ากลัวเลย

คุณเสง - เดชฤทธิ์ สีหาราช

EDC ถือเป็นหลักสูตรที่ยกระดับทักษะและศักยภาพทางด้านดิจิทัล ทั้ง 5 ด้าน ให้กับตัวผู้ได้เป็นอย่างดี สามารถนำเอาไปต่อยอดได้ในชีวิตประจำวัน ซึ่งสอดรับกับสถานการณ์ของโลกในยุคปัจจุบัน ที่เปลี่ยนแปลงไป

คำนิยม



EDC TRAINER รุ่น 2

คุณตึก - ศิริรัตน์ กุญชรจันทร์



ขอขอบคุณโครงการ EDC Trainer ที่ได้จัดขึ้นมาเพื่อหาแนวร่วมในการช่วยกันส่งต่อความรู้ ความเข้าใจในการใช้สื่ออย่างปลอดภัย และเป็นประโยชน์ ต่อสังคมอย่างมาก ช่วยยกระดับคุณภาพชีวิตของประชาชนและสร้างความยั่งยืนให้กับพลเมืองในยุคดิจิทัลนี้

คุณต้อง - สุมนต์ จิรพัฒนพร



อบรม EDC แล้ว เมื่อต้องส่งต่อความรู้ต่อไปผ่านเบรียบตัวผู้ให้เป็นเหมือน GPS ที่ค่อยแนะนำเส้นทางในการใช้งานด้านดิจิทัล ได้ถูกต้องเหมาะสม รู้ทันก้าวทันโลก ช่วยให้คนไทยไม่หลงทางในยุคดิจิทัล

คุณแพร - ณิชา บุตรดีสุวรรณ



ในฐานะข้าราชการครู ได้นำความรู้ที่ได้มาใช้ในการจัดการเรียนรู้ เช่น การใช้สื่อดิจิทัล หรือ Digital Footprint ให้กับนักเรียน รวมถึงทักษะการใช้ชีวิตที่สอดคล้องกับการจัดการเรียนรู้ในศตวรรษที่ 21 ให้รู้เท่าทันในการ “เลือกรับ” และ “ปรับใช้” ข้อมูลสารสนเทศที่มีอยู่อย่างเหมาะสม

สารบัญ

ด้านที่ 1 อัตลักษณ์ดิจิทัล (Digital Identity)	1
1.1 Digital Citizen Identity	7
เพราะทุกคนล้วนมีโลกอิเล็กทรอนิกส์	8
แล้วอะไรคือสิ่งที่แสดงตัวตนของเราในโลกดิจิทัล ?	9
รู้ได้อย่างไร ใครเป็นเจ้าของอัตลักษณ์ ?	11
Biometrics สิ่งที่ใช้แยกแยะตัวตนของแต่ละบุคคล	12
อัตลักษณ์ดิจิทัลในทางบวก = อัตลักษณ์ทางบวกในชีวิตจริง	13
ผลกระทบจากการสร้างอัตลักษณ์ทางดิจิทัล	14
How to 3 STEP ในการปรับปรุงอัตลักษณ์ดิจิทัล	16
สรุปแล้วปัง ! คณาฯ 8 ข้อ เสริมชีวิต สร้างอัตลักษณ์ดิจิทัลที่ดี ในสังคมดิจิทัล	18
BEST PRACTICES แนวทางปฏิบัติที่ดีในการจัดการอัตลักษณ์ดิจิทัล	19
1.2 Digital Privacy	23
ความเป็นส่วนตัวในโลกดิจิทัล (สิ่งมีค่าที่เราอาจหลงลืมไป)	24
รู้ทันภัย และความเสี่ยง หากไม่ดูแลข้อมูลส่วนตัวให้ดี	26
ปัญหาภัยคุกคามและละเมิดความเป็นส่วนตัว	28
การจัดการความเป็นส่วนตัวในโลกดิจิทัล	32
กฎหมายที่น่าสนใจ และควรรู้ไว้	39

สารบัญ

ด้านที่ 2 การใช้เทคโนโลยีดิจิทัลอย่างเหมาะสม (Digital Use)	47
2.1 Balanced Use of Technology การใช้เทคโนโลยีอย่างมีความสมดุล	53
การดูแลสุขภาพบนโลกดิจิทัล (Digital Health)	57
การบริหารจัดการเวลาบนโลกดิจิทัล (Screen Time Management)	68
การมีส่วนร่วมอย่างสร้างสรรค์ในชุมชนดิจิทัล	83
2.2 Civic Use of Technology การใช้เทคโนโลยีเพื่อสังคมและตนเอง	87
การใช้เทคโนโลยีในโลกดิจิทัลเพื่อสังคมและตนเอง	88
การใช้เทคโนโลยีอย่างเหมาะสม เพื่อสร้างค่านิยมเชิงบวกต่อชุมชนและพัฒนา คุณภาพชีวิต	98
การสืบค้นข้อมูลจากสื่อดิจิทัล	104
ด้านที่ 3 การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security)	119
3.1 Behavioral Cyber-Risk Management	125
การล่วงละเมิดทางไซเบอร์ (Cyber Abuse)	128
ภัยคุกคามทางไซเบอร์ (Cyber Threat)	133
ออนไลน์อย่างไรให้ปลอดภัย	142
3.2 Organizational Cyber-Risk Management	151
ความเสี่ยงจากการใช้เทคโนโลยีในองค์กร	153
แนวปฏิบัติเพื่อร่วมกันป้องกันภัยไซเบอร์ระดับองค์กร	159

สารบัญ

ด้านที่ 4 การสื่อสารดิจิทัล (Digital Communication)	169
4.1 Digital Footprint Management	175
เครื่องมือในการจัดการ Digital Footprint	180
ร่องรอยดิจิทัลเชิงบวกและเชิงลบ	181
4.2 Interaction & Collaboration	193
ทักษะพื้นฐานสื่อสารอย่างเข้าใจ	194
การเลือกใช้เทคโนโลยีเพื่อการสื่อสารอย่างสร้างสรรค์	195
ปัจจัยที่ทำให้การสื่อสารประสบความสำเร็จหรือล้มเหลว	196
การรับมือกับประเด็นสื่อสารทางลบ	198
4.3 Future Skill สำหรับการสื่อสาร	205
ทักษะสำคัญแห่งยุคดิจิทัล	206
มารยาทในโลกดิจิทัล (Netiquette)	209
สิ่งที่ควรปฏิบัติในการสื่อสารบนโลกดิจิทัล	211
มารยาทในการประชุมออนไลน์	213
4.4 Cyberbully	217
การสื่อสารเครื่องมือสำคัญในการป้องสิทธิดิจิทัล	218
คนทำไม่เคยจะ แต่ผู้ถูกกระทำการลับไม่เคยลืม	219
การจัดการกับ Cyberbully	224
วิธีการรับมือกับการกลั่นแกล้งทางไซเบอร์	227

สารบัญ

ด้านที่ 5 การรู้เท่ากันดิจิทัล (Digital Literacy)	235
5.1 Media & Information	241
รู้เท่าทันดิจิทัลทักษะจำเป็นเพื่อชีวิตออนไลน์	242
ธรรมชาติของสื่อ	250
การประเมินคุณภาพและความน่าเชื่อถือของข้อมูลจากสื่อดิจิทัล	253
แนวทางในการรับชมสื่อย่างรู้เท่าทัน	262
ศิลปะแห่งการจัดการข้อมูลจากสื่อดิจิทัลด้วยตนเอง	264
5.2 Digital Content Creation	275
สื่อและเนื้อหาดิจิทัล	276
การสร้างเนื้อหาดิจิทัลให้ดึงดูดและเกิดการจดจำ	283
หลักการสร้างเนื้อหาให้ถูกกฎหมายและมีจริยธรรม	285
ลิขสิทธิ์ กับ Creative Commons	289
การอ้างอิงแหล่งข้อมูล (Citation) ในงานวิจัย	298
5.3 Data & AI Governance	307
เท่าทัน AI เทคโนโลยีเพื่ออนาคต	308
โอกาสและความท้าทายจาก AI	310
การใช้ AI ในชีวิตประจำวัน	312
ความเสี่ยงจากการใช้เทคโนโลยี AI	318
อนาคตของ AI	331

01



อัตลักษณ์ดิจิทัล



Digital Identity

ແນະນຳສໍາຮັບຜູ້ສວນ



- **ວັດຖຸປະສົງຄົມ**

ຜູ້ເຮັດວຽກມີຄວາມຮູ້ ແລະ ສາມາດອອນໄບຍ່າງຄື່ງ ຄວາມສໍາຄັງຂອງອັຕລັກຊົນດິຈິຫຼັດ ດັ່ງນີ້ແມ່ນມີຄວາມຮູ້ ແລະ ສາມາດອອນໄບຍ່າງຄື່ງ ຂອງອັຕລັກຊົນດິຈິຫຼັດ

- **ຂອບເຂດຂອງເນື່ອຫາດ້ານນີ້**

1.1 Digital Citizen Identity

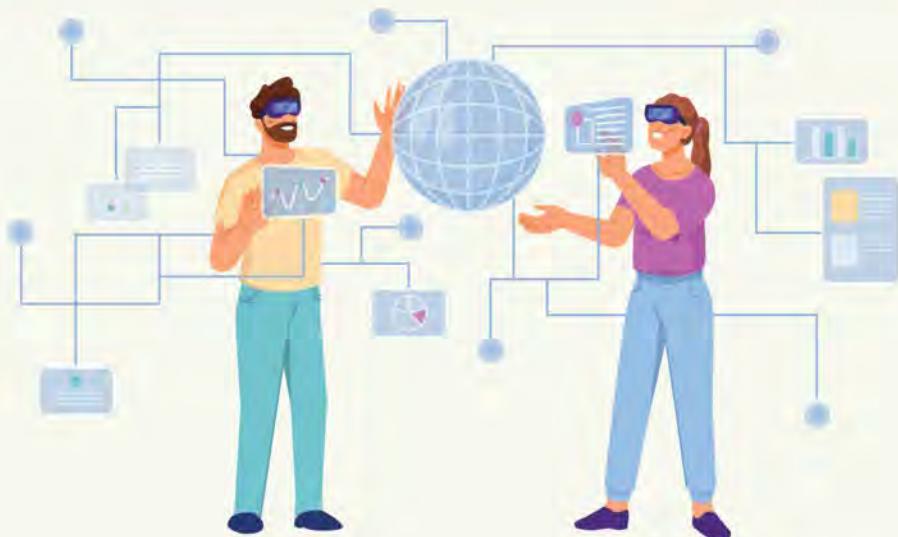
- ໂຄດິຈິຫຼັດ ວັນທີສອນ
/...../
- ອັຕລັກຊົນດິຈິຫຼັດຄືອະໄຣ ? ວັນທີສອນ
/...../
- ກະບວນກາງກາරຮະບຸຕ້າວນ ພິສູຈົນ ແລະ ຍືນຍັນຕ້າວນ ວັນທີສອນ
/...../
- Biometrics ສິ່ງທີ່ໃຊ້ແຍກແຍະຕ້າວນຂອງແຕ່ລະບຸຄຸຄລ ວັນທີສອນ
/...../
- ການສ້າງອັຕລັກຊົນດິຈິຫຼັດ ວັນທີສອນ
/...../
- ພັດຈາກການສ້າງອັຕລັກຊົນທາງດິຈິຫຼັດ ວັນທີສອນ
/...../
- ການປັບປຸງ ແລະ ແນວປົງປົມທີ່ດີໃນການຈັດການອັຕລັກຊົນດິຈິຫຼັດ ວັນທີສອນ
/...../

● ขอบเขตของเนื้อหาด้านนี้

1.2 Digital Privacy

- ความเป็นส่วนตัวในโลกดิจิทัล วันที่สอน
/ / / /
- รู้ทันภัย และความเสี่ยง หากไม่ดูแลข้อมูลส่วนตัวให้ดี วันที่สอน
/ / / /
- การจัดการความเป็นส่วนตัวในโลกดิจิทัล วันที่สอน
/ / / /
- กฎหมายที่น่าสนใจ และควรรู้ไว้ วันที่สอน
/ / / /

เวลาในการเรียน



รู้ศัพท์ ไม่สับสน



1



TOXIC SOCIETY

สภาพแวดล้อมทางสังคมที่มักจะมีการกระทำ
ความคิด หรือการแสดงออก ที่ส่งผลต่อ
คนในสังคม ซึ่งอาจจะส่งผลกระทบต่อสุขภาพ
สภาพจิตใจ ความสัมพันธ์ ตลอดจนคุณภาพชีวิต
โดยอาจจะเกิดจากการไม่ให้เกียรติผู้อื่น
การแข่งขันที่ไม่สร้างสรรค์ การมองโลกในแง่ร้าย
หรือการปิดกันความคิดเห็นของผู้อื่น

2



TWO-FACTOR AUTHENTICATION

การเข้าสู่ระบบด้วยการยืนยันตัวตน
แบบ 2 ชั้น 2 ขั้นตอน โดยขั้นตอนแรกคือ
การใส่อีเมลและรหัสผ่านตามปกติ
และขั้นตอนที่ 2 คือ เพิ่มกระบวนการยืนยันตัวตน
ผ่านอีเมลสำรอง เบอร์โทรศัพท์ หรือการสแกน
ลายนิ้วมือ หรือวิธีการต่าง ๆ

3



ONE-TIME PASSWORD : OTP

ชุดรหัสผ่านที่สามารถใช้ได้เพียงครั้งเดียว
ต่อการเข้าสู่ระบบหนึ่งครั้ง หากกรอกรหัสผิด
หรือกรอกข้าข้าวเวลากำหนด
การเข้าระบบนั้น ก็จะไม่สำเร็จ

4



ROMANCE SCAM

คือ การหลอกให้หลงรัก หลอกให้เชื่อว่ารัก
หลอกให้เชื่อใจ และใช้ความรักความเชื่อใจ
หรือความหวังของเหยื่อ เพื่อแสวงหาประโยชน์

รู้ศัพท์ ไม่สับสน



5



HYBRID SCAM

คือ การหลอกลวงที่ผสมผสานระหว่าง
ความรัก และการลงทุน
หลอกให้เชื่อใจ ไว้ใจ แล้วชวนลงทุน

6



REMOTE ACCESS SCAM

คือ หลอกให้รักแล้วกดลิ้งก์ ดาวน์โหลด
แอปพลิเคชันรีโมต ควบคุมสมาร์ตโฟน
และการดูดเงินในบัญชี

7



SEXTORTION

การขู่กรรไชทางเพศ เมื่อต้นด้วยการ
เข้ามาขอเป็นเพื่อนผ่านช่องทางต่าง ๆ
และชวนทำกิจกรรมทางเพศผ่านทางออนไลน์
จากนั้น มิจฉาชีพจะบันทึกภาพ วิดีโอดังกล่าวไว้
แล้วนำมายั่นชุบภายหลัง



ถ้าคุณเรียนผ่านด้านนี้
คุณจะสามารถ
รักษาได้ทั้งข้อมูลส่วนตัว
และ ทรัพย์สิน

1.1

DIGITAL CITIZEN IDENTITY

วัตถุประสงค์

- ผู้เรียนอธิบายถึงการสร้างอัตลักษณ์ดิจิทัลของตนเองให้เหมาะสมได้
- ผู้เรียนตระหนักถึงความสำคัญของอัตลักษณ์ดิจิทัล
- ผู้เรียนตระหนักถึงผลกระทบที่จะเกิดขึ้นจากการสร้างอัตลักษณ์ดิจิทัล ทั้งเชิงบวกและลบได้
- ผู้เรียนสามารถเข้าใจถึงพฤติกรรมที่แสดงออกถึงการมีจริยธรรมในโลกดิจิทัลได้





เราทุกคน ล้วนมีโลกอีกใบ

รู้หรือไม่ ?

REMEMBER

“เราทุกคนล้วนมีโลกอีกใบ” ประโยชน์นี้ พังดูแล้ว ก็อาจชวนสร้างรอยร้าวให้กับหลายบ้านได้ แต่สำหรับบริบทนี้ โลกอีกใบ ที่กำลังหมายถึงคือ โลกเสมือน ที่เราทุกคนสร้างขึ้นมาคู่ขนานกับโลกความจริงที่เรารอยู่อาศัยหรือเรียกว่า “โลกดิจิทัล” โดยโลกใบนี้ จะประกอบด้วยพื้นที่ ผู้คน เครื่องมือ ทรัพยากร และกิจกรรมที่คล้ายกับโลกความจริง เพียงแต่ถูกสร้างขึ้นจากอุปกรณ์อิเล็กทรอนิกส์ และดำเนินชีพผ่านออนไลน์นั่นเอง ซึ่งก่อนที่เราจะเป็นพลเมือง หรือผู้คนในโลกดิจิทัลได้นั้น เราต้องทำการสมัครเข้าใช้งานยอมรับเงื่อนไขในการเข้าสู่พื้นที่แต่ละแห่งในโลกดิจิทัลก่อน เพื่อให้เรามีตัวตนบนโลกใบนี้ แล้วจึงจะสามารถสร้าง หรือทำกิจกรรมต่าง ๆ ได้ ไม่ว่าจะเป็น

ติดต่อสื่อสาร



แบ่งปัน
ข้อมูลข่าวสาร

ใช้บริการ
หน่วยงานภาครัฐ
และเอกชน



ทำธุรกรรม
ทางการเงิน



อะไรคือ สิ่งที่แสดงตัวตน ของเรานในโลกดิจิทัล ?



REMEMBER

เมื่อเรารอการสร้างชีวิตขึ้นมาอยู่บนโลกดิจิทัลแล้วนั้น อีกคำถามที่ตามมาคือ “แล้วอะไรคือ สิ่งที่แสดงออกถึงตัวตนของเรา เมื่อยูในโลกดิจิทัล ?” สิ่งนั้นเรียกว่า อัตลักษณ์ดิจิทัล หรือสิ่งที่บ่งบอกความเป็นตัวเรา ลักษณะเฉพาะบุคคลของเรา และภาพลักษณ์ที่แสดงออกให้ผู้อื่นรับรู้ ซึ่งเกิดจากข้อมูลที่ใส่หรือโพสต์ลงบนโลกดิจิทัล โดยหากใครพบเห็น ก็จะสามารถจดจำ และใช้ระบุตัวตนของเราได้

3 องค์ประกอบหลัก ปักหมุดอัตลักษณ์ดิจิทัล

ข้อมูลเกี่ยวกับอัตลักษณ์ดิจิทัลของเรา เรียกได้ว่าแทบจะเป็นข้อมูลเดียวกันกับข้อมูลบนโลกความเป็นจริงเลยก็ว่าได้ เพราะสามารถเชื่อมโยงข้อมูลเหล่านี้เข้าด้วยกัน เพื่อระบุถึงตัวของเราได้ โดยแบ่งเป็น 3 องค์ประกอบหลัก ดังนี้

1

Personal Information (PII)

1.1 Linked Information

ข้อมูลที่สามารถเชื่อมโยงให้รับรู้ได้โดยทันทีว่าเป็นเรา เช่น ชื่อ-นามสกุล ที่อยู่ เบอร์โทรศัพท์ อีเมล รูปภาพประจำตัว เลขใบขับขี่ เลขบัตรเครดิต เลขบัตรประชาชน เลขพาสปอร์ต

1.2 Linkable Information

ข้อมูลที่เชื่อมโยงถึงตัวเราได้ เมื่อนำข้อมูลมาประกอบกัน เช่น ชื่อ หรือ นามสกุล ชื่อเล่น ตำแหน่งที่อยู่ ประเทศ รหัสไปรษณีย์ เพศ ผ่านพันธุ์ เชื้อชาติ กลุ่มอายุ อาชีพ ประวัติการทำงาน การศึกษา วันเดือนปีเกิด

2

Social & Behavioral Information

ข้อมูลทางสังคม และข้อมูลเชิงพฤติกรรมการใช้งาน เช่น ความสัมพันธ์กับบุคคลอื่น ความสนใจ ทัศนคติ พฤติกรรม ลักษณะนิสัย การแสดงออก

3

Digital Information

ข้อมูลทางดิจิทัล เช่น บัญชีและรหัสผ่านแพลตฟอร์มต่าง ๆ ประวัติการใช้งานอินเทอร์เน็ต ข้อมูลการเข้าถึงเว็บไซต์ โพสต์บนโซเชียลมีเดีย

รู้ได้อย่างไร ให้เป็น เจ้าของอัตโนมัติ ?



การจะบอกได้ว่า ใครคือเจ้าของอัตโนมัตินั้น ควรที่จะผ่านกระบวนการ
การระบุตัวตน พิสูจน์ และยืนยันตัวตนที่มีระดับความน่าเชื่อถือก่อน

การระบุตัวตน (Identification)



คือขั้นตอนที่ผู้ใช้แสดงตนว่าเป็นใคร มีอัตลักษณ์ดิจิทัลได เช่น การกรอก
ชื่อผู้ใช้

พิสูจน์ตัวตน (Identity Proofing)



คือ ขั้นตอนรวม แล้วตรวจสอบความเชื่อมโยงระหว่างบุคคลกับ
อัตลักษณ์นั้น เพื่อให้มั่นใจว่าอัตลักษณ์นั้นเป็นของคนนั้นจริง

ยืนยันตัวตน (Authentication)



คือขั้นตอนการยืนยันอัตลักษณ์ของบุคคล ด้วยการตรวจสอบสิ่งที่ใช้ยืนยัน
ตัวตน เช่น รหัสผ่าน OTP Biometrics เป็นต้น



Biometrics

สิ่งที่ใช้แยกแยะตัวตนของแต่ละบุคคล

โดยในปัจจุบัน หากต้องการวัดลักษณะเฉพาะ เพื่อแยกแยะ และระบุตัวตนของแต่ละบุคคลสามารถทำได้ด้วยเทคโนโลยี ไบโอมิตริก (Biometrics) ซึ่งแบ่งการวัดเป็น 2 ลักษณะ คือ

1 ลักษณะทางสรีริทยา (Physiological Characteristics)

เป็นสิ่งที่มองเห็นได้โดยตรงจากส่วนต่าง ๆ ของร่างกาย เช่น ใบหน้า ม่านตา ลายนิ้วมือ ดีเอ็นเอ (DNA)



ลักษณะทางสรีริทยานั้น มักจะถูกนำมาใช้ในระบบการพิสูจน์ตัวตน (Identify) เพื่อยืนยันว่าเราเป็นบุคคลนั้นจริง ๆ เช่น การเปิดบัญชี หรือทำธุรกรรมทางการเงินบนแอปพลิเคชัน ที่ใช้การใช้ใบหน้า หรือลายนิ้วมือในการยืนยันตัวตน

2

ลักษณะเฉพาะทางพฤติกรรม (Behavioral Characteristics)

เป็นสิ่งที่วัดจากการกระทำ หรือพฤติกรรมการแสดงออกของแต่ละบุคคล เช่น เสียงพูด ลายเซ็น ลักษณะการเดิน การพูด

อัตลักษณ์ดิจิทัลในทางบวก = อัตลักษณ์ทางบวกในเชิงต่อต้าน

จะเห็นได้ว่า อัตลักษณ์ดิจิทัลนี้ เป็นสิ่งสำคัญในอย่างมากในการใช้ชีวิตบนโลกดิจิทัลของเรา ดังนั้น เราจึงควรมีการสร้างอัตลักษณ์ดิจิทัลที่ดี ทั้ง 3 องค์ประกอบ

① Personally Identifiable Information

เน้นการดูแล ปกป้องให้ปลอดภัย เพื่อป้องกันไม่ให้เสี่ยงโดนสวมรอยโดยไม่ตัวตนจากบุคคลอื่น เช่น ไม้பேஸ்ட์เปิดเผยข้อมูลส่วนบุคคลต่าง ๆ ที่สำคัญในอินเทอร์เน็ต หรือให้ข้อมูลกับบุคคลที่ไม่น่าเชื่อถือ หรือควรตั้งค่าความเป็นส่วนตัวในบัญชีออนไลน์ต่าง ๆ เพื่อจำกัดวงผู้อ่าน หรือนำข้อมูลไปใช้

② Social & Behavioral Information

เน้นการสร้างสรรค์ และแสดงออกอย่างเหมาะสม

③ Digital Information

เน้นการจัดการอย่างปลอดภัย ไม่เข้าเว็บไซต์ที่ไม่น่าเชื่อถือ เว็บพนันหรือเว็บอโกจ์ ไม่สร้างร่องรอยดิจิทัลอันด่างพร้อย

ผลจากการสร้าง อัตลักษณ์ทางดิจิทัล



ผลลัพธ์

สุดว้าว การสร้างอัตลักษณ์ดิจิทัลที่ดี



01

ภาพจำที่แสนเลิศ



ผู้คนจะจำเราในทางที่ดี เพราะการจำในทางที่ดีจะส่งผลต่อการใช้ชีวิตในโลกความเป็นจริง ทั้งในปัจจุบัน และอนาคต

เปิดโอกาสให้ตัวเอง

02



หากเราสร้างเนื้อหาที่ดีที่ผู้คนชื่นชอบจนใจฟูก็จะมีคนเข้ามาติดตามเรามากขึ้น สิ่งนี้เปิดโอกาสให้พวกรามากมาย ตั้งแต่ได้รับการชื่นชม ได้มีโอกาสเข้าร่วมกิจกรรมใหม่ ๆ สร้างสังคมใหม่ ๆ หรืออาจนำไปสู่การสร้างรายได้ในรูปแบบของ Content Creator ได้

เป็นบ้านสังคมดิจิทัลที่น่าอยู่

03



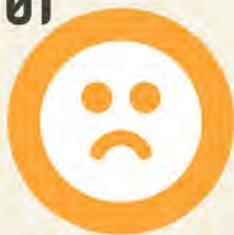
สร้างสภาพแวดล้อมบนโลกออนไลน์ ในเชิงสร้างสรรค์ ช่วยเหลือและสอดส่องภัยที่เกิดขึ้น ทำให้ลดปัญหาการโจกรรรมทางดิจิทัล สะท้อนผลกระทบในเชิงบวกกลับมายังโลกของความเป็นจริงและยังช่วยลดภาวะการเกิด Toxic Society ด้วย

ในทางตรงกันข้าม หากเราสร้างอัตลักษณ์ดิจิทัลในทางลบ ก็อาจส่งผล ดังนี้

ผลกระทบ

แบบทรง จำกอัวต์ลักษณ์ดิจิทัลในทางลบ

01



ติดลบด้วยภาพจำ

การถูกจดจำในทางที่ไม่ดี อาจส่งผลเสียมากกว่าที่คิด ตั้งแต่ ปัญหาด้านภาพลักษณ์ ความสัมพันธ์ จนไปถึงโอกาสในหน้าที่การทำงาน และความน่าเชื่อถือ เช่น ในกรณีนักศึกษาฝึกงาน ได้โพสต์ข้อความด้วยอารมณ์ว่า สถานที่เคยฝึกงานไว้ จึงไม่ได้รับพิจารณาจากที่ทำงาน ที่ไปสมัครงาน เพราะถูกตัดสินจากโพสต์ ที่สะท้อนทัศนคติและบุคลิกภาพโดยอิสระ

02



สุดข้าความสัมพันธ์

หากเราสร้างอัตลักษณ์ที่ไม่ดี อาจส่งผลต่อความรู้สึกของคนรอบข้าง เกิดความขัดแย้ง ไม่พอใจกับสิ่งที่เราโพสต์ แซร์ หรือเผยแพร่ ไปจนถึงอาจเกิดการระรานในโลกดิจิทัลผ่านช่องทางต่าง ๆ ด้วยการใช้ถ้อยคำเสียดสี จนทำให้เกิดความไม่สงบภายใน

03



รู้ไม่กัน ภูกใจกรรมข้อมูล

หากเราเผยแพร่ข้อมูล หรือเก็บรักษาอัตลักษณ์ไม่ดี ผู้ประสงค์ร้าย หรือมิจฉาชีพอาจใช้อัตลักษณ์ของเราในการโจมตีข้อมูล หลอกลวง หรือละเมิดความเป็นส่วนตัว



มาจัดการ อัตโนมัติทั้งหมด !

ก่อนอื่นถ้าหากเราจำไม่ได้ว่า เราเคยทำอะไร ที่จะทำให้เกิด อัตโนมัติทั้งหมดที่ไม่ได้ไว้หรือไม่ ? ให้ลองมาตรวจสอบด้วยวิธีนี้

How to 3 STEP

ในการปรับปรุงอัตโนมัติทั้งหมด

- STEP 1**  **ค้นหาชื่อ และข้อมูลบนโลกดิจิทัล**
ให้พิมพ์ชื่อจริง หรือชื่อ Account ที่ต้องการค้นหา บน Google
- STEP 2**  **ลบข้อมูลด้วยตัวเองง่ายนิดเดียว**
ไม่ต้องหาอัตโนมัติทั้งหมดที่ไม่ต้องการให้คุณอื่นเห็น จากผลลัพธ์ที่ขึ้นมา จากนั้นเข้าไปทำการลบ หากไม่สามารถดำเนินการลบได้ด้วยตัวเอง ให้ทำการกด รีโพร์ต หรือติดต่อเข้าไปที่ผู้ดูแล หรือผู้ให้บริการ เพื่อติดต่อขอความช่วยเหลือ
- STEP 3**  **เริ่มต้นใหม่ ใส่ใจอัตโนมัติ**
เมื่อรู้แล้วว่า ต้องมีอะไรผิดพลาดตรงไหน ควรทำความเข้าใจ หลีกเลี่ยงไม่ให้เกิดขึ้นอีกครั้ง และสร้างอัตโนมัติทั้งหมดต่อจากนี้ให้ดี



ชีວຕາກີ່ດີ ເຮັມຈາກສັງຄມທີ່ນ່າວຍູ້

ໃນຍາມທີ່ເຮັນນັ້ນ ມີຕົວຕະບຸນໂລກໄມ່ວ່າຈະເປັນໂລກຄວາມຈິງ ອ້າວໂລກດິຈິຫຼັດ ເຮັຍ່ອມຄື່ອເປັນສາຂຶກຄນໜຶ່ງໃນສັງຄມ ເປັນພລມື່ອງໃນສັງຄມນັ້ນ ແລະ ສັງຄມ ຈະເປັນເຊັ່ນໄຣ ກີ່ຍ່ອມສ່າງຜລຕ່ອຄຸນພາພ່ອວິດຂອງເຮົາດ້ວຍ ດັ່ງນັ້ນ ທັກເຮາ ອີກາມມີຄຸນພາພ່ອວິດທີ່ດີ ເຮົາກີ່ຄວາມມີຄວາມເຂົ້າໃຈ ແລະ ປັບປຸງຕິດໃຫ້ແໜ້ນສົມ ເພື່ອສ້າງສັງຄມໃຫ້ນ່າວຍູ້ໄປດ້ວຍກັນ ອ້າວໂລກດິຈິຫຼັດ ອາຈໝາຍຄື່ງ ການມີຈິຍຮຽນພລມື່ອງດິຈິຫຼັດ ນັ້ນເອງ





TIP

สวัสดีแล้วปัง !



คากา 8 ข้อ เสริมชีวิต สร้างอัตลักษณ์ดิจิทัลที่ดี

1. คิดก่อนโพสต์

ควรเน้นการโพสต์แชร์ข้อมูลหรือเนื้อหาที่สร้างสรรค์และมีประโยชน์

2. มีประโยชน์กึ่งแชร์

คิดให้ดีก่อนโพสต์และแชร์เพื่อสร้างภาพจำที่ดีในโลกดิจิทัล

3. ถูกลิ้นแม่อย่าใจร้อน

ไม่ใจร้อน ตอบกลับด้วยอารมณ์คิดให้รอบคอบก่อนตอบโต้

4. ใช้ตัวอักษรตัวอักษร

ทุกอย่างในโลกออนไลน์มีเจ้าของ จึงต้องระมัดระวังในการนำข้อมูลที่ไม่รู้ที่มาหรือไม่ได้รับอนุญาตไปใช้งาน หากจำเป็นควรมีการอ้างอิง หรือการขออนุญาตก่อนการใช้งาน

5. ไม่ย่อหย่อน กฎหมาย

ปฏิบัติตามกฎหมายทางปฏิบัติของชุมชนออนไลน์ เช่น กรณีการเข้าร่วมกลุ่มผ่านโซเชียลมีเดียต่าง ๆ ควรปฏิบัติการแนวทางที่แต่ละกลุ่มได้กำหนดไว้

6. ทุก ๆ คนควรให้เกียรติ

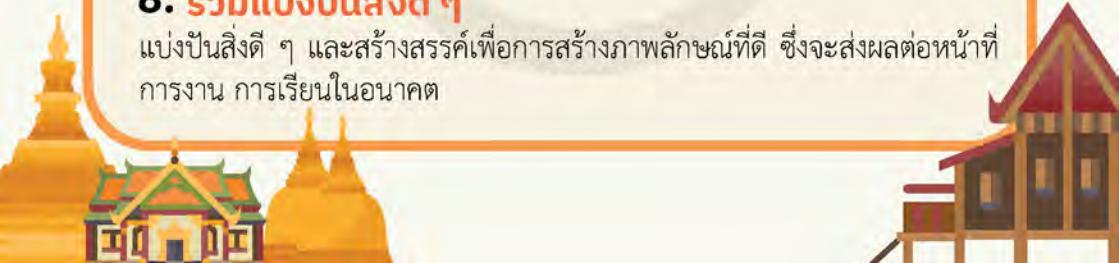
ให้เกียรติเคารพความคิดเห็นของผู้อื่น โดยไม่เลือกว่า เป็นใคร ช่วงอายุใด เพศใด หรือทำอาชีพอะไร

7. อย่าเรียกกัวร์ความขัดแย้ง

ระมัดระวังในการแชร์หรือโพสต์ข้อมูลที่อาจทำให้เกิดความขัดแย้ง หรือกระทบกับความรู้สึก โดยเฉพาะเนื้อหาที่เกี่ยวกับความเชื่อ วัฒนธรรม และการเมือง

8. ร่วมแบ่งปันสิ่งดี ๆ

แบ่งปันสิ่งดี ๆ และสร้างสรรค์เพื่อการสร้างภาพลักษณ์ที่ดี ซึ่งจะส่งผลต่อหน้าที่การงาน การเรียนในอนาคต





TIP

BEST PRACTICES

แนวปฏิบัติที่ดีในการจัดการ อัตลักษณ์ดิจิทัล



1



ชื่อ - นามสกุล

ใช้ชื่อ姓名สกุลที่ไม่ทำให้
ผู้อื่นเสียหาย และไม่ควรใช้
ชื่อ姓名สกุลของผู้อื่น

2



รูปภาพประจำตัว

ไม่ใช้ภาพของผู้อื่นมาเป็น
รูปภาพประจำตัว
หรือภาพที่ละเมิดผู้อื่น

3



ข้อมูลส่วนตัว

ตั้งค่าความเป็นส่วนตัว
ไม่เผยแพร่ข้อมูล
ที่ไม่ควรเผยแพร่

4



ประวัติในการใช้งาน

ตรวจสอบประวัติ
การใช้งานบนโลกออนไลน์
เป็นระยะ หลีกเลี่ยงการเข้าถึง
เนื้อหาที่ไม่เหมาะสมในอนาคต

5



เนื้อหา ข้อความ รูปภาพที่เผยแพร่

ตรวจสอบก่อน
ว่าถูกต้องหรือสร้าง
ความเสียหายหรือไม่

6



สถานที่เช็คอิน

หากพบว่าได้เช็คอินในสถานที่
ที่กระทบต่ออัตลักษณ์
ให้ลบ หลีกเลี่ยงการเช็คอิน
สถานที่ที่ไม่เหมาะสม

7



กลุ่มหรือสังคม ที่เราเข้าร่วม

ตรวจสอบกลุ่มที่เข้าร่วม
หากมีเนื้อหาหรือกิจกรรม
ที่กระทบต่ออัตลักษณ์
ให้ทำการออกจากกลุ่ม
และหลีกเลี่ยงการเข้าร่วม
กลุ่มที่ไม่เหมาะสม

8



เพื่อน บุคคล องค์กรที่เราติดตาม

ตรวจสอบบุคคลที่รับเป็นเพื่อน
หรือขอเป็นเพื่อน
หากเป็นบุคคลที่เราไม่ต้องการ
ให้รับรู้เรื่องราว ให้ทำการ
ยกเลิกขอเป็นเพื่อน
หรือยกเลิกการติดตาม

9



ความคิดเห็น ในโซเชียลมีเดีย

ตรวจสอบการแสดง
ความคิดเห็นในโซเชียลมีเดีย¹
หลีกเลี่ยงการแสดง
ความคิดเห็นที่ไม่เหมาะสม





ดั่งโลกนี้มีอิกใบใช้ชีวิต

เนรมิตตัวตนดิจิทัล

คู่ขنانกับโลกจริงผูกชีวัน

รู้จักกันอัตแล็กษณ์บอกตัวตน

ดังนั้นควรเสริมสร้างภาพที่ดี

ทำให้มีรากศีลัwanเป็นผล

แต่ถ้าหากไม่ระวังน่ากังวล

จะยกตนควรพินิจคิดให้ดี



ถ้าคุณเรียนผ่านด้านนี้
คุณจะเข้าใจความสำคัญ
ของความเป็นส่วนตัว
และป้องกันภัยคุกคาม
ในโลกดิจิทัลได้



1.2

DIGITAL PRIVACY

วัตถุประสงค์

- ผู้เรียนตระหนักรึถึงความสำคัญของความเป็นส่วนตัว
- ผู้เรียนสามารถเข้าใจถึงการจัดการข้อมูลส่วนตัวในโลกดิจิทัลได้
- ผู้เรียนมีความรู้เกี่ยวกับกฎหมายที่เกี่ยวข้อง
- ผู้เรียนสามารถเข้าใจถึงการแก้ไขปัญหาภาวะคุกคามหรือละเมิดความเป็นส่วนตัว





สิ่งมีค่า ที่เราอาจหลงลืมไป

การใช้ชีวิตในโลกดิจิทัลนั้น บางครั้งเราก็ลืมห่วงเห็นในสิ่งที่เราเห็นคุณค่า ในโลกความจริง สิ่งนั้นเรียกว่า "ความเป็นส่วนตัว" เราราย堙มหลบเลี่ยง การถูกคนข้าง ๆ ชะเง้อส่องจอมือถือ เราไม่ชอบให้ใครมาแกะกล่องพัสดุ ที่ส่งมาที่บ้าน หรือเราก็เลือกปิดม่าน ปิดประตู เพื่อรักษาพื้นที่ส่วนตัว แต่ หลายคนบนโลกออนไลน์ ก็กลับกลายเปิดเผยชีวิตทุกซอกทุกมุม และเปิด ช่องโหว่ให้คนแพลกหน้า เข้ามาติดตามสอดส่องได้อย่างหายใจดันคอ โดยไม่รู้ตัว และแน่นอนว่า หากเราไม่รักษาความเป็นส่วนตัวให้ดี สิ่งที่เรา ต้องแลกับการไม่ดูแลสิ่งมีค่านี้ ก็มีตั้งแต่การถูกกลเม็ด ถูกแอบอ้าง ถูก สมรอย ไปจนถึงการต้องรับผิดชอบในสิ่งที่ไม่ได้ก่อ และบางรายอาจ นำไปสู่การเสียทรัพย์สิน หรือเสียชีวิตได้ ดังนั้น เราจึงต้องมีการควบคุม การเผยแพร่ข้อมูล หรือใช้สิทธิในข้อมูลที่เกี่ยวข้องกับตัวเรา ไม่ยินยอมให้ คนที่เราไม่อนุญาต นำข้อมูลนั้นไปถือครองหรือใช้ประโยชน์ นี่คือ "การปกป้องความเป็นส่วนตัว"



WARNING



REMEMBER

Digital Privacy หรือ "ความเป็นส่วนตัวในโลกดิจิทัล" จึงหมายถึง เป็นสิทธิในการเป็นเจ้าของควบคุม ข้อมูลส่วนตัว และเนื้อหาที่เราสร้างขึ้น รวมไปถึง พื้นที่ทางดิจิทัลส่วนตัว ในการเปิดเผยหรือเผยแพร่ข้อมูลใด ๆ ให้กับผู้อื่น

โดยข้อมูลส่วนตัวบางข้อมูลเรามาตรฐานเปิดเผยได้ (Personal Information) เช่น ชื่อเล่น นามแฝง อายุ เพศ อาหารที่ชอบ หนังเรื่องโปรด ชื่อสัตว์เลี้ยง

แต่เมื่อข้อมูลบางอย่างที่มีความสำคัญกับความปลอดภัย ที่ไม่ควรเผยแพร่ให้เป็นสาธารณะ (Private Information) เช่น ชื่อจริง นามสกุลจริง เลขบัตรประจำตัวประชาชน เลขบัญชีธนาคาร ที่อยู่ หมายเลขโทรศัพท์ อีเมล ชื่อผู้ใช้งาน และรหัสผ่านต่าง ๆ



WARNING

รู้กันภัยและความเสี่ยง หากไม่ดูแลข้อมูลส่วนตัวให้ดี

โปรดอ่าน ! ก้าไม่อยากเสี่ยง

ลักษณะของความเสี่ยง

ที่อาจจะเกิดขึ้น หากไม่ดูแลข้อมูลส่วนตัวให้ดี อาจเสี่ยงจากการถูกโจกรกรรม ข้อมูล การถูกหลอกลวง และการถูกกลั่นเมิดความเป็นส่วนตัวได้ เช่น การนำ ข้อมูลบนเฟซบุ๊กของเราไปแอบอ้าง เพื่อหลอกให้เพื่อนหรือญาติเราโอนเงิน ให้ หรือเอาข้อมูลเราไปใช้เพื่อหลอก Romance Scam

EXAMPLE

ยกตัวอย่างข่าว เตือนภัยคนโสด ระวังถูกหลอกให้รักแล้วโอนเงิน



นายประเสริฐ จันทร์วงศ์ รมว. ดิจิทัลเพื่อเศรษฐกิจและสังคม หรือ ดีอี กล่าวว่า ขอให้ระวังภัยที่อาจจะเกิดขึ้นจากการหลอกให้รักและโอนเงินออนไลน์ (Romance Scam) ในรูปแบบต่าง ๆ เช่น มิจฉาชีพเข้ามาทักทายผ่านโซเชียลมีเดีย จากนั้น ขอคุณเป็นเพื่อนและคนรัก

EXAMPLE

ยกตัวอย่างข่าว เตือนภัยคนโสด ระวังถูกหลอกให้รักแล้วโอนเงิน

ก่อนที่จะขอให้เหยื่อโอนเงินให้พร้อมหลอกเหยื่อว่า มีความจำเป็นต้องใช้เงินในรูปแบบต่าง ๆ โดยเฉพาะคนโสด ซึ่งจะตกเป็นเป้าหมายของมิจฉาชีพได้ง่าย ผ่านการล่อหลวงให้รัก โดยการใช้เทคนิคทางจิตวิทยา สร้างความเชื่อใจระหว่างกัน พอร์กแล้วจะชวนลงทุน (Hybrid Scam) ชวนกดลิงก์ หรือดาวน์โหลดแอปฯ รีโมต (Remote Access Scam) ดูดเงินในบัญชี หรือหลอกให้รักแล้วแบล็กเมล (Sextortion) ขู่กรีซทางเพศ เป็นต้น

“ล่าสุดพูดติกรรมยังขยายไปถึง การหลอกให้กดรับสติกเกอร์วันวาเลนไทน์พรี หลอกหลวงให้ผู้ใช้ไลน์ใส่ชื่อและรหัสการเข้าใช้ไลน์ รวมถึง ข้อมูลส่วนตัว แล้ว นำชื่อ และรหัสการใช้งานของเหยื่อไปทำธุกรรมต่าง ๆ หรืออาจมีการ สวมสิทธิ์เพื่อกระทำผิด”

นายประเสริฐ กล่าวอีกว่า จากตัวเลขของศูนย์บริหารรับแจ้งความออนไลน์ สำนักงานตำรวจแห่งชาติ ที่มีการเก็บสถิติตัวเลขคดีหลอกให้รักและโอนเงินออนไลน์ ระหว่าง 1 มี.ค. 65 - 31 ม.ค. 67 หรือในรอบ 1 ปี 11 เดือน พบร่วม มีคดีที่เกิดขึ้นเกี่ยวกับ Romance Scam จำนวน 3,323 คดี มีความเสียหายมากกว่า 1,154 ล้านบาท คิดเฉลี่ยความเสียหาย คดีละประมาณ 34,752 บาท นับว่าเป็นการสูญเสียจำนวนไม่น้อยเลย

ปัญหาภัยคุกคาม

และ

ละเมิดความเป็นส่วนตัว



ในปัจจุบัน มีปัญหาภัยคุกคามความเป็นส่วนตัวทางดิจิทัลในหลากหลายรูปแบบ ดังนี้

1 การลวงให้กดยินยอมหรือตอบรับ

ขั้นตอนแรก ๆ เมื่อติดตั้งแอปพลิเคชัน หรือ สมัครใช้บริการดิจิทัล มักจะมีขั้นตอนการให้กดยินยอม ตกลง อนุญาต ตอบรับ ซึ่งบางครั้งมาในรูปแบบที่ผู้ใช้ไม่ทันได้ตั้งใจพิจารณา เช่น เป็นกล่องข้อความขนาดเล็ก เป็นข้อความเงื่อนไขขนาดยาว เป็นปุ่มที่ง่ายต่อการกดอนุญาต หรือ ยินยอม ซึ่งบางครั้งอาจเป็นกลลวงเพื่อขอกำหนดให้ผู้ใช้ เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น และอาจถูกนำข้อมูลเหล่านั้นไปใช้ในทางมิชอบ เช่น แอปฯ เงินกู้ขอเข้าถึงอัลบัมรูปภาพและสมุดรายชื่อ

2 การหลอกให้กรอกข้อมูลส่วนตัว

เครื่องมือสำคัญที่ใช้ในการหลอกลวง อาจเป็นเทคนิคการสร้างข่าวปลอม เว็บปลอม ข้อมูลวงที่ดูน่าเชื่อ เพียงเพื่อให้เราลงเชื่อแล้วกรอกข้อมูล ส่วนตัวหรืออนุญาตให้เข้าถึง เช่น การแอบอ้างว่าเป็นแบบฟอร์มขอรับเงินจากโครงการของรัฐบาล เป็นต้น

3 ทำให้ดีใจ ตกใจ หวาดกลัว ก่อนจะจ่าย ข้อมูลส่วนตัว



บางครั้งมีข้อความสั้นๆ ส่งมาพร้อมลิงก์ ซึ่งบางคนเห็นแล้วก็อาจจะตกใจและรีบเร่งเข้าไปดำเนินการ โดยไม่ทันได้ตระหนักรู้ว่าเป็นกับดักของมิจฉาชีพ

4 ภาคธุรกิจจะเมิด หรือใช้ข้อมูลส่วนตัวผิด วัตถุประสงค์

ผู้ให้บริการบางรายไม่ปฏิบัติตามมาตรฐาน และกฎหมายการคุ้มครองข้อมูลส่วนบุคคล อาจมีการนำข้อมูลส่วนตัวของเราไปขายต่อ หรือนำไปใช้ผิดวัตถุประสงค์ที่เรายินยอมหรืออนุญาตตั้งแต่ต้น ซึ่งอาจนำมาซึ่งการถูกคุกคามหรือก่อความรำคาญได้

EXAMPLE

จากข่าวเรื่อง เตือน ! ระวังแก๊งมิจฉาชีพ แอบอ้าง สปส. หลอกโอนเงิน-ขโมยข้อมูลส่วนตัว



นายบุญสุข ท้าพชัยยุทธ์ เลขาธิการสำนักงานประกันสังคม กระทรวงแรงงาน ได้ประชาสัมพันธ์เตือนประชาชน เกี่ยวกับแก๊งมิจฉาชีพที่ได้แอบอ้างสำนักงานประกันสังคม สร้างเว็บไซต์และเพจปลอม เพื่อหลอกให้ผู้ประกันตนกดลิงก์และขอข้อมูลส่วนตัวและนำไปสวมรอยทำธุรกรรมจนสูญเสียทรัพย์สิน รวมถึง ก่ออาชญากรรมอื่น ๆ ซึ่งอาจทำให้เกิดความเดือดร้อนและยุ่งยากภายหลัง

EXAMPLE

WHOSCALL รายงานประจำปี 2566 คนไทยเป็นเหยื่อ SMS หลอกลวงมากที่สุดในเอเชีย



Whoscall ผู้นำด้านแอปพลิเคชันระบุตัวตนสายเรียกเข้าที่ไม่รู้จัก และป้องกันสแปม สำหรับสมาร์ตโฟน เผยรายงานประจำปี 2566 พบมิจฉาชีพก่อการคนไทยเพิ่มขึ้น 12.2 ล้านครั้ง คนไทยรับข้อความหลอกลวงมากที่สุดในเอเชียถึง 58 ล้านข้อความ ซึ่งแนบมา กับลิงก์ปลอมลิงก์ขออินบลอก อีเมล โทรเดมัลแวร์ อันตราย และเพจปลอมหลอกขายของหลอกลวง

คนไทยรับ SMS หลอกลวงมากที่สุดในเอเชีย

Whoscall เผยจำนวนข้อความหลอกลวง เฉลี่ยคนไทย 1 คน ต้องรับ SMS ที่ น่าสังสัย 20.3 ข้อความ ซึ่งมากที่สุดในเอเชีย โดยอันดับ 2 คือพิลิปปินส์ จำนวน 19.3 ข้อความ และอ่อนลง จำนวน 16.2 ข้อความ แนวโน้มดังกล่าวแสดงให้เห็นว่าปัญหานี้ กำลังเพิ่มขึ้นในภูมิภาค ทำให้เจ้าหน้าที่และผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ พยายามเตือนให้ประชาชนเพิ่มความระมัดระวัง เพื่อป้องกันการหลอกลวงและความเสี่ยงที่อาจทำให้สูญเสียเงิน

มารู้จักจัดการความเป็นส่วนตัว ก่อนต้องใช้คำว่า รู้จึ่ง... !

การจัดการความเป็นส่วนตัวในโลกดิจิทัล

1 ไม่เผยแพร่ข้อมูลส่วนตัว

ที่มีความสำคัญกับตัวเราให้เป็นสาธารณะ



2 จำกัดการเข้าถึงหรือการมองเห็นข้อมูล

เพื่อลดโอกาสการเข้าถึงข้อมูลของคนที่ประสงค์ร้าย



3 จัดการอุปกรณ์ให้มีความปลอดภัย

ให้ตั้งค่าการตรวจสอบสิทธิ์ 2 ขั้นตอน หรือ Two - Factor Authentication (2FA) เช่น การส่งข้อความรหัส Code มาให้กรอกเพิ่มนอกเหนือจากการใส่ หรือใช้รหัสยืนยันต่อการเข้าสู่ระบบแต่ละครั้ง (One-time Password : OTP) หรือการยืนยันตัวตนด้วยลายนิ้วมือหรือใบหน้า



4 คิดและอ่าน ก่อนกดตกลงหรือยืนยом

ทำความเข้าใจเงื่อนไขหรือข้อตกลงที่แอปพลิเคชัน หรือโปรแกรมร้องขอเข้าถึงข้อมูลส่วนตัว หากอ่านแบบผ่านแล้วกดยอมรับไป ข้อมูลส่วนตัวของเราอาจถูกนำไปใช้ตักตวงผลประโยชน์และถูกละเมิดได้โดยไม่รู้ตัว



5 ตั้งรหัสผ่านให้มีความปลอดภัย

ไม่ใช้รหัสเดียวกันทุกบัญชีในทุกแพลตฟอร์ม ถ้ารู้สึกสงสัยว่า ถูกแฮกให้เปลี่ยนรหัสผ่านใหม่ทันที และหากกังวลว่าจะจำไม่ได้ สามารถใช้ฟังก์ชัน “ลืมรหัสผ่าน” ได้ นอกจากนั้น ในขณะนี้บางหน่วยงานเริ่มมีการนำมาตรฐานเทคโนโลยีใหม่ มาใช้แทนรหัสผ่าน เรียกว่า Passkey ซึ่งจะช่วยให้เราไม่ต้องยุ่งยากกับการจดจำรหัสผ่าน และยังปลอดภัยยิ่งขึ้นอีกด้วย



(ติดตามได้ในด้านที่ 3 Digital Security เรื่องออนไลน์อย่างไรให้ปลอดภัย)

การจัดการข้อมูลส่วนตัวสำหรับผู้ให้บริการ

ในส่วนของผู้ให้บริการก็จะต้องมีมาตรฐานในการจัดการข้อมูลส่วนตัวของเรา ด้วยเช่นกัน โดยมีหลักการสำคัญ 4 ข้อ คือ

1 การยืนยัน (Authentication)

ความสามารถในการตรวจสอบว่าเป็นบุคคลนั้นจริง อาจดูได้จากบัตรประชาชน การพิสูจน์ลายนิ้วมือ หรือการพิสูจน์ด้วยรหัสผ่าน



2 ความสมบูรณ์ (Integrity)

ความสามารถในการรักษาข้อมูลให้ถูกต้องและไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต



3 ความลับ (Confidentiality)

ความสามารถในการป้องกันไม่ให้บุคคลที่ไม่เกี่ยวข้องสามารถเข้าถึงข้อมูลได้



3 การเข้าถึง (Availability)

ความสามารถในการทำให้เข้าถึงหรือใช้งานข้อมูลและบริการพร้อมใช้งานเมื่อต้องการ เช่น การพิสูจน์ตัวตน การเข้ารหัส



ทั้งหมดนี้คือสิ่งสำคัญที่เราควรต้องคำนึงถึง เมื่อต้องเลือกส่งมอบข้อมูลส่วนตัว อันมีค่า ไว้ในครองของผู้ใด และขณะเดียวกัน ผู้ให้บริการนั้น ก็จะต้องมีระบบการพิสูจน์และยืนยันตัวตนที่เข้มแข็งรักษาด้วย

**TIP**

โดยระบบยืนยันตัวตนที่ได้รับความนิยม และมีความปลอดภัย มี 2 ระบบ ด้วยกัน คือ KYC และ E-KYC

KYC กระบวนการทำความรู้จักบุลลอกดิจิทัล หรือ Know Your Customer แปลตรงตัวว่า¹ "ทำความรู้จักลูกค้าของคุณ"

แต่ในทางดิจิทัล จะหมายถึง กระบวนการระบุตัวตน - พิสูจน์ตัวตน - ยืนยันตัวตน ของลูกค้าได้อย่างถูกต้อง ซึ่งถือเป็นหลักเกณฑ์สำคัญหนึ่ง ของ พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ที่กำหนดให้ เป็นหน้าที่ของหน่วยงาน เช่น ธนาคารผู้ให้บริการ e-Wallet e-Payment บริษัทซื้อขายหลักทรัพย์ บริษัทประกัน หรือเรียกว่าเป็นกระบวนการที่จะ ทำให้ผู้ให้บริการมั่นใจได้ว่า ผู้ที่กำลังติดต่ออยู่นั้น คือ บุคคลนั้นจริง ๆ นั่นเอง

E-KYC ย่อมาจากคำว่า “Electronic Know Your Customer” หรือเรียกสั้น ๆ ว่า “E-KYC”

คือกระบวนการที่ใช้เทคโนโลยีดิจิทัลในการยืนยันและตรวจสอบความถูกต้อง ของข้อมูล และตัวตนของลูกค้าในรูปแบบอิเล็กทรอนิกส์ ซึ่งใช้ประโยชน์ใน การตรวจสอบและยืนยันตัวตนของลูกค้าอย่างรวดเร็วและปลอดภัยยิ่งขึ้น

โดยรูปแบบ E-KYC มักใช้ในรูปออนไลน์ หรือแอปพลิเคชันที่ผู้ใช้บริการสามารถกรอกข้อมูลส่วนตัว และเอกสารประจำตัวอย่างบัตรประชาชน หรือหลักฐานอื่น ๆ และส่งข้อมูลเหล่านั้นไปยังผู้ให้บริการ หรือหน่วยงานที่ต้องการใช้งานได้เลย

ซึ่งในความเป็นจริงแล้ว เมื่อเราติดต่อสื่อสารกับครอบโนล็อกดิจิทัล หรือผ่านอุปกรณ์สื่อสาร เรายังคงมีการพิสูจน์และยืนยันตัวตนบุคคลเหล่านั้นให้แน่ใจก่อนเสมอ เพื่อไม่ให้ตกเป็นเหยื่อผู้ที่สวมรอย อย่างน้อยเมื่อเราต้องกรอกข้อมูลส่วนตัว ข้อมูลทางการเงิน หรือต้องมีการโอนเงิน หรือดาวน์โหลดแอปฯ ใด ๆ มาติดตั้ง



TIP

5 ทริค

เสริมเกราะป้องกันภัยคุกความเป็นส่วนตัว

1

ปกป้องอุปกรณ์ของตัวเอง



เช่น ตั้งค่าความเป็นส่วนตัว ไม่กดยินยอมอนุญาตโดยไม่รู้ และไม่ต้องการ สร้างรหัสผ่านที่รักกุม อัปเดตระบบปฏิบัติการในอุปกรณ์ให้มีความทันสมัยอยู่เสมอ

2



หมั่นอัปเดตกลโกงที่เกิดขึ้นผ่านช่องทางต่างๆ

ทั้งออนไลน์และออฟไลน์ หากเกิดขึ้นกับตัวเองต้องมีสติ และรู้เท่าหัน รวมถึงการมีแหล่งข้อมูล เพื่อการแจ้งกรณีพบเหตุการณ์ไม่พึงประสงค์ทางออนไลน์ ซึ่งอาจจะส่งผลกระทบต่อตัวเราเองและผู้อื่น

3



คิดให้ดีก่อนโพสต์หรือตอบกลับข้อความ

ควรหันมาสนใจว่าสิ่งที่เราโพสต์ไม่สามารถลบออกจากอินเทอร์เน็ตได้อย่างสมบูรณ์

4



เมื่อต้องซื้อสินค้าหรือบริการผ่านทางออนไลน์

ควรเลือกใช้ช่องทางที่น่าเชื่อถือ และสามารถติดตามความหายความรับผิดชอบในภายหลังได้

5



ระวังการบันทึกข้อมูลจากการเงินบนเว็บไซต์ที่ไม่รู้จัก

เพราะอาจเสียถูกข้อมูล เช่น เลขที่บัญชีธนาคาร หมายเลขบัตรเครดิต ไปใช้ในทางที่ผิดได้

EXAMPLE**ยกตัวอย่าง**

ช่องทางติดตามข่าวสาร และแจ้งเหตุ



ศูนย์รับแจ้งความอ่อนไลน์ว่าชุมชนกรรมทางเทคโนโลยี

ผ่าน www.thaipoliceonline.go.th และ ศูนย์ AOC 1441

สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.)

รับเรื่องร้องทุกข์ และช่วยเหลือผู้บริโภคที่ไม่ได้รับความเป็นธรรมจากการซื้อสินค้า และบริการ ติดต่อขอคำปรึกษาทาง สคบ.1166 หรือร้องทุกข์ผ่าน <https://complaint.ocpb.go.th>

ศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์ หรือ 1212 ETDA

รับเรื่องร้องเรียนให้แก่ผู้บริโภคหรือผู้ประกอบการทั้งภาครัฐ และเอกชน ทั้งในเรื่องเว็บไซต์พิดกฤษามัย ปัญหาชี้ช่องออนไลน์ ปัญหาภัยคุกคามไซเบอร์ และแจ้งปัญหาอื่น ๆ โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ สพอ. (ETDA) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

- 1212 (24 ชั่วโมง)
- 1212@mdes.go.th
- www.1212ETDA.com
- [@1212etda](http://facebook.com/1212ETDA)

ศูนย์ชัวร์ก่อนแชร์ สำนักข่าวไทย -osmth

หน่วยงานด้านการเสริมสร้างความรู้เท่าทัน ตรวจสอบข้อเท็จจริงเรื่องที่แชร์กันบนโซเชียล

: @SureAndShare หรือ <http://line.sure.guru>



กฎหมายที่นำเสนอด้วย และควรรู้ไว้



พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562
หรือ กฎหมาย PDPA

ย่อมาจาก Personal Data Protection Act

คือ กฎหมายที่กำหนดให้องค์กรหรือหน่วยงานที่จัดเก็บและจัดการข้อมูล
ส่วนบุคคลของประชาชน ไม่ว่ารัฐหรือเอกชน จะต้องได้รับความยินยอม
ในการเข้าถึง จัดเก็บ จัดการ และคุ้มครองดูแลข้อมูลเหล่านั้น และไม่นำ^{ไปใช้ในกิจกรรมที่เราไม่ยินยอม}



บทลงโทษของ PDPA

- โทษทางอาญา จำคุกไม่เกิน 1 ปี และ/หรือ ปรับสูงสุด 1 ล้านบาท
โทษทางแพ่ง จ่ายสินไหมไม่เกิน 2 เท่าของสินไหมที่แท้จริง
- โทษทางปกครองปรับไม่เกิน 5 ล้านบาท


REMEMBER

ข้อมูลส่วนบุคคล หมายถึงอะไรบ้าง ?

ข้อมูลส่วนตัว

หมายถึง ข้อมูลที่สามารถระบุตัวตนเจ้าของข้อมูลได้ เช่น

ชื่อ - นามสกุล

ที่อยู่

เบอร์โทรศัพท์

E-mail

เลขบัตรประชาชน

ข้อมูลส่วนบุคคลที่มีความอ่อนไหว

เชื้อชาติ

ความเห็นทางการเมือง

ความเชื่อ

ศาสนา

พฤติกรรมทางเพศ

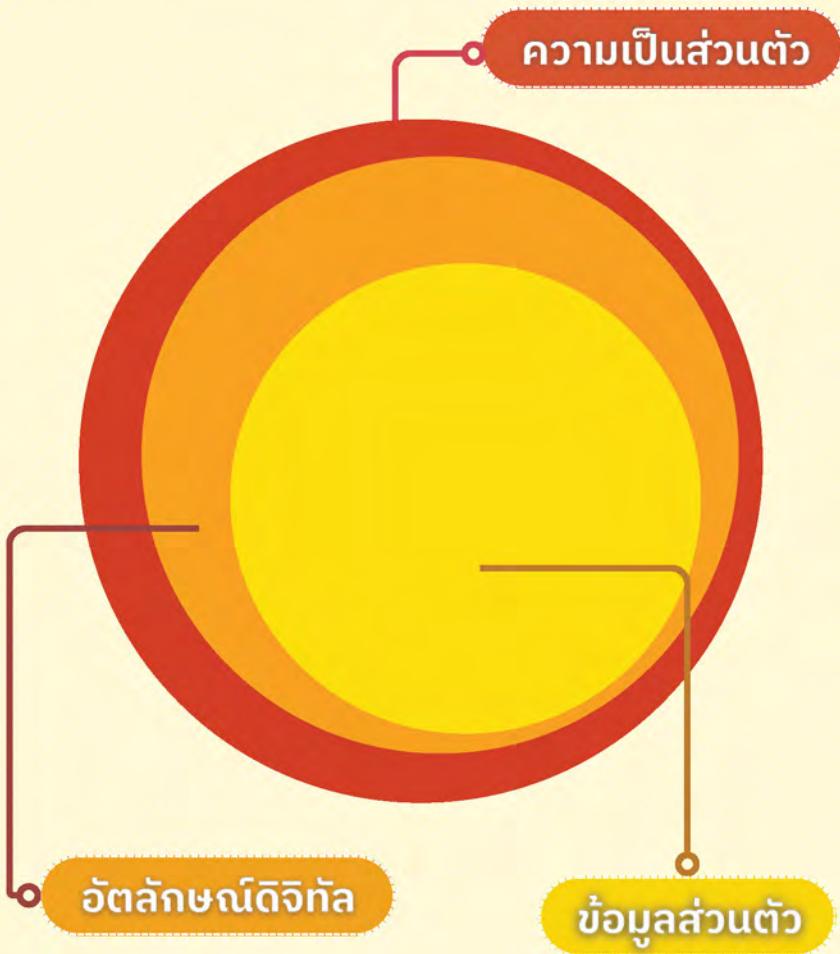
ประวัติอาชญากรรม

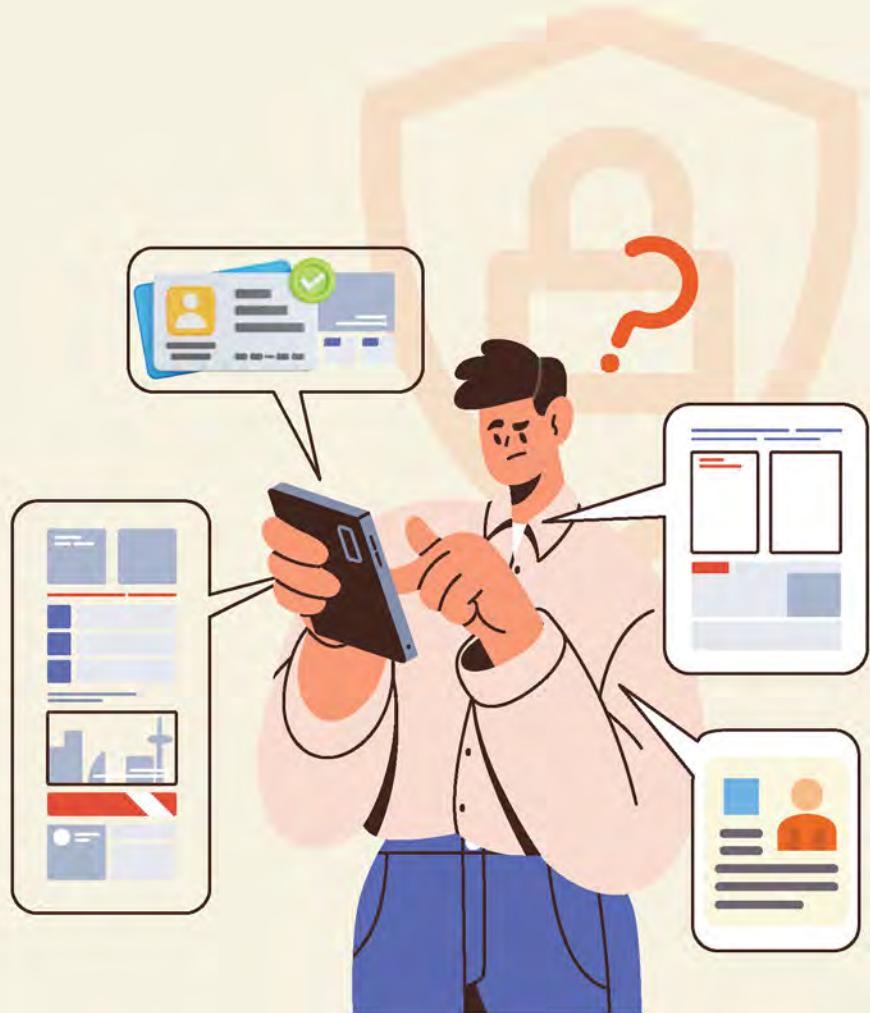
ข้อมูลทางด้านสุขภาพ

ข้อมูลชีวภาพ

ความสัมพันธ์ระหว่าง

อัตลักษณ์ ความเป็นส่วนตัว และข้อมูลส่วนตัว







เราทุกคนล้วนมีเขตทางห้าม
 เสมือนความเป็นส่วนตัวต้องรักษา
 เพราะข้อมูลส่วนตัวบอกชีวा
 ที่ไม่น่าเผยแพร่ควรเก็บ紧
 หึ้งซื้อเช่าเลขบัตรแล้วันเกิด
 ถ้าไปเปิดอาจเตลิดโดนรุกถ้า
 เสียชื่อเสียงเสียทรัพย์สุดระกำ
 จะไม่ชำถ้าปกป้องไว้ให้ดี

เพราะทุกคน
 ล้วนมาโลกอีกใบ

กิจกรรมต่าง ๆ
 ในโลกดิจิทัล

ติดต่อสื่อสาร

ใช้บริการหน่วยงาน
 ภาครัฐและเอกชน

แบ่งปันข้อมูลข่าวสาร

ทำธุกรรมทางการเงิน

Biometrics

สิ่งที่ใช้แยกแยะตัวตน
 ของแต่ละบุคคล

ลักษณะทางสรีริวิทยา

ลักษณะเฉพาะทาง
 พฤติกรรม

ผลจากการสร้าง
 อัตลักษณ์ทางดิจิทัล

ผลลัพธ์สุดท้าย

ผลกรรมเสบthrw

1.1

Digital Citizen Identity

รู้ได้อย่างไร
 ใครเป็น
 เจ้าของอัตลักษณ์?

อะไรคือ สิ่งที่
 แสดงตัวตน
 ของเราในโลกดิจิทัล ?

3 องค์ประกอบหลัก
 ปักหมุดอัตลักษณ์ดิจิทัล

Personal
 Information (PII)

Social & Behavioral
 Information

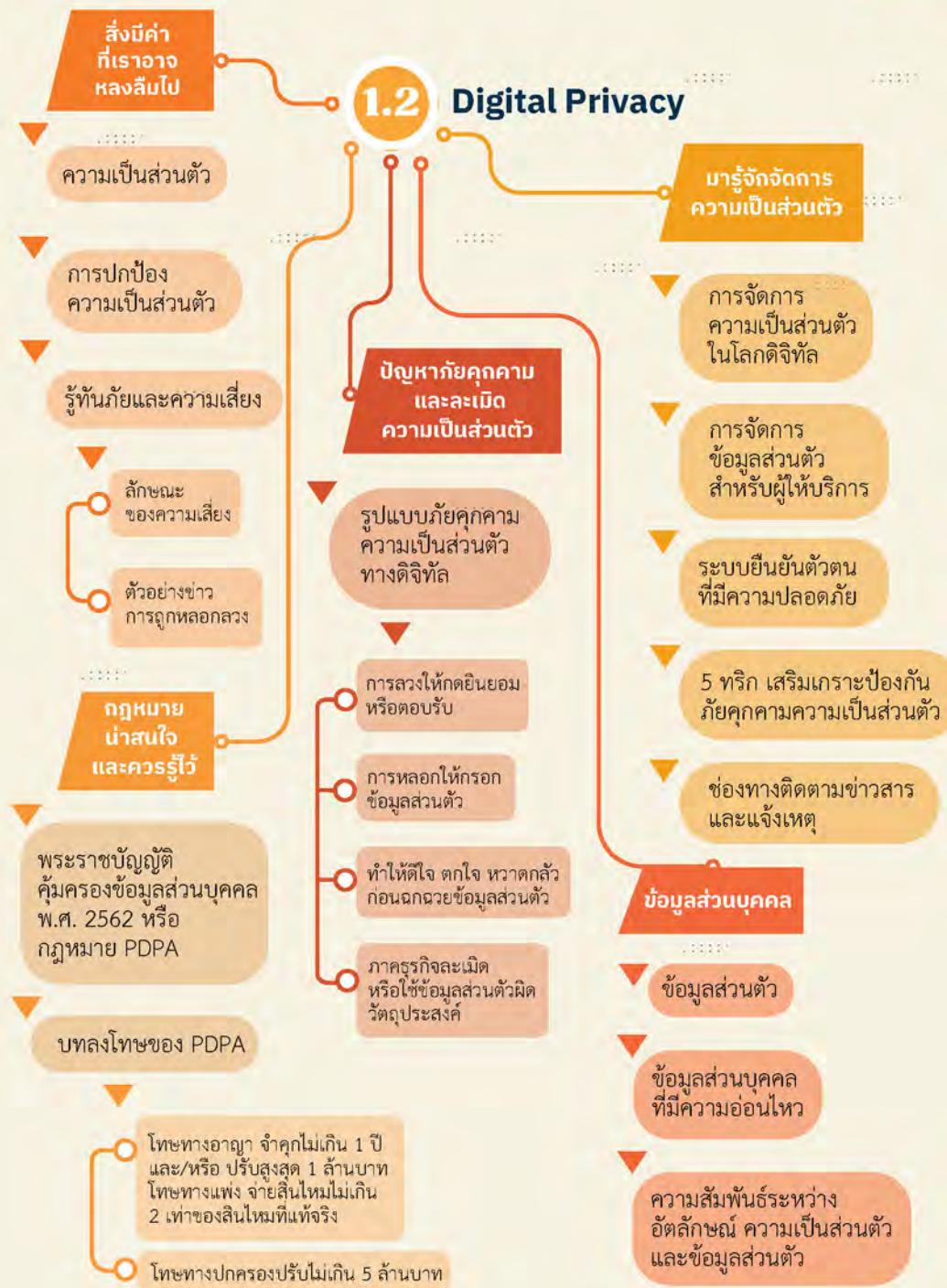
Digital
 Information

การถูแล
 อัตลักษณ์ดิจิทัล

How to 3 STEP
 ในการปรับปรุงอัตลักษณ์ดิจิทัล

ค่าถูก 8 ข้อ เสริมชีวิต
 สร้างอัตลักษณ์ดิจิทัลที่ดี

แนวปฏิบัติที่ดีในการจัดการ
 อัตลักษณ์ดิจิทัล



02



การใช้เทคโนโลยีดิจิทัล อย่างเหมาะสม

— Digital Use —

ແນະນຳສໍາຫຼັບຜູ້ສວນ



• ວັດຖະການ

ຜູ້ເຮັດວຽກມີຄວາມຮູ້ເກີຍກັບການຄັ້ງຫາ ຮົບຮົມ ແລະ ຈັດກາຮັບຂໍ້ມູນທີ່ຕ້ອງກາຮັບຈາກສື່ອດິຈິທັລ ອົບຍາຍຄືການແປ່ງເວລາສໍາຫຼັບກາຮັບໃຊ້ເທັກໂນໂລຢີທີ່ເໝາະສົມແລະ ຜຸດກະຮົບທີ່ເກີດຂຶ້ນໄດ້

• ຂອບເຂດຂອງເນື່ອຫາດ້ານນີ້

2.1 Balanced Use of Technology ກາຮັບໃຊ້ເທັກໂນໂລຢີ ອົບຍາຍມີຄວາມສົມດຸລ



ກາຮັບຜູ້ສໍາຫຼັບຜູ້ສໍາຫຼັບສົມດຸລ ໂດຍໃຊ້ເທັກໂນໂລຢີ

ວັນທີສອນ
...../...../.....



ກາຮັບຜູ້ສໍາຫຼັບຜູ້ສໍາຫຼັບສົມດຸລ ໂດຍໃຊ້ເທັກໂນໂລຢີ

ວັນທີສອນ
...../...../.....



ກາຮັບຜູ້ສໍາຫຼັບຜູ້ສໍາຫຼັບສົມດຸລ ໂດຍໃຊ້ເທັກໂນໂລຢີ

ວັນທີສອນ
...../...../.....

● ขอบเขตของเนื้อหาด้านนี้

2.2 Civic Use of Technology การใช้เทคโนโลยี

เพื่อสังคมและตนเอง



การใช้เทคโนโลยีในโลกดิจิทัลเพื่อสังคมและตนเอง

วันที่สอน

...../...../.....



การใช้เทคโนโลยีอย่างเหมาะสมเพื่อสร้างค่านิยมเชิงบวกต่อชุมชน

และพัฒนาคุณภาพชีวิต

วันที่สอน

...../...../.....



การสืบค้นข้อมูลจากสื่อดิจิทัล

วันที่สอน

...../...../.....

เวลาในการเรียน



รู้คัพก ไม่สับสน



1



ERGONOMICS

คือ วิทยาการเพื่อการทำงาน โดยให้วิทยาศาสตร์ เข้ามายोงสัมพันธ์กับเนื้องาน บุคลากร สภาพแวดล้อม เพื่อออกแบบลักษณะ ของการทำงานให้มีประสิทธิภาพ ลดความเสี่ยงผลกระทบ ต่อสุขภาพหรืออันตรายจากอุบัติเหตุ

2



DIGITAL HEALTH

คือ การดูแลสุขภาพและความเป็นอยู่ที่ดี ในยุคดิจิทัล โดยมุ่งเน้นการใช้เทคโนโลยี อุปกรณ์และสมุด เพื่อส่งเสริมสุขภาพ ทั้งทางร่างกาย จิตใจ และการดำเนินชีวิตโดยรวม

3



PHYSICAL HEALTH

คือ สภาพความสมบูรณ์ของร่างกาย

4



MENTAL HEALTH

คือ สภาพความสมดุลของจิตใจ อารมณ์ สังคม และจิตวิญญาณ ซึ่งมีผลต่อการตัดสินใจ หรือ แก้ปัญหาต่าง ๆ

รู้คัพก ไม่สับสน



5



SCREEN TIME

คือ คำที่ใช้เรียกวิจกรรมต่าง ๆ
บนหน้าจอดิจิทัล

6



CONTENT ADDICTION

หรือ การเสพติดเนื้อหา
คือ เป็นภาวะติดการเสพข้อมูล
หรือน้ำหนานสื่อดิจิทัล ทำให้เกิดผลกระทบ
กับการทำงาน การเรียน และการขาดปฏิสัมพันธ์
กับคนรอบข้างอย่างเห็นได้ชัด

7



DIGITAL WELLBEING

หรือ สุขภาวะดิจิทัล
คือ การใช้เทคโนโลยีดิจิทัลในเชิงบวก
เพื่อส่งเสริมสุขภาพกาย สุขภาพจิต
และความเป็นอยู่ที่ดี โดยไม่ให้ส่งผลเสีย
ต่อชีวิตประจำวันและมีสุขภาพที่ดี



ถ้าคุณเรียนผ่านด้านนี้
คุณจะไม่เสี่ยงเป็น
โรคออฟพิศซินโดรม
รวมถึงโรคติดจอได้

2.1

BALANCED USE OF TECHNOLOGY

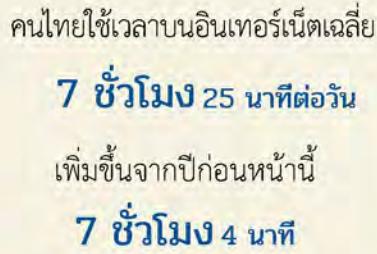
วัตถุประสงค์

- ผู้เรียนอธิบายถึงการแบ่งเวลา ในการใช้เทคโนโลยีโดยคำนึงถึงผลกระทบต่อสุขภาพ การทำงาน สุขภาวะ การดำเนินชีวิตประจำวันได้
- ผู้เรียนสามารถเลือกและใช้เครื่องมือหรืออุปกรณ์หรือเทคโนโลยีที่ส่งผลดีต่อสุขภาพ (ERGONOMICS) ได้
- ผู้เรียนสามารถเข้าใจถึงการจัดการ และตั้งค่าการเข้าถึงเนื้อหา ที่เหมาะสม เพื่อป้องกันการเสพติดเนื้อหาที่มีผลกระทบต่อสุขภาพจิตของตนเอง



เทคโนโลยีพัฒนาอย่างรวดเร็ว ส่งผลให้พฤติกรรมการใช้เทคโนโลยีของคนไทยมีแนวโน้มเปลี่ยนแปลงไปอย่างต่อเนื่อง โดยเทคโนโลยีดิจิทัลเข้ามามีบทบาทสำคัญในชีวิตประจำวันของคนไทยมากขึ้น ไม่ว่าจะเป็นการใช้เพื่อการสื่อสาร การทำงาน การเรียน การศึกษาหาความรู้ และความบันเทิง

จากผลสำรวจพฤติกรรมการใช้อินเทอร์เน็ตของคนไทยในปี 2566 โดยสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สศช.) พบว่า



กิจกรรมที่คนไทยนิยมทำบนอินเทอร์เน็ต ได้แก่ รับชมวิดีโอคอนเทนต์ พูดคุยบนบล็อกและกระดูก โอนเงินผ่านเว็บไซต์ ช้อปปิ้งออนไลน์ และสื่อสารความบันเทิงในโลกออนไลน์



พฤติกรรมการใช้เทคโนโลยีที่เปลี่ยนแปลงไปนี้ ส่งผลดีต่อคนไทยในหลายด้าน เช่น



- ช่วยให้สามารถเข้าถึงข้อมูลและข่าวสารได้อย่างรวดเร็วและทันเหตุการณ์
- ช่วยให้สามารถทำงานและเรียนหนังสือจากที่บ้านได้



- ช่วยให้สามารถติดต่อสื่อสารกับผู้อื่นที่อยู่ห่างไกลได้
- ช่วยให้สามารถเข้าถึงความบันเทิงและความรู้ได้หลากหลายรูปแบบ

อย่างไรก็ตาม ความเพลิดเพลินจากการใช้เทคโนโลยีที่มากเกินไป ก็อาจส่งผลเสียต่อร่างกาย จิตใจ และชีวิตประจำวันได้เช่นกัน อาทิ



- เกิดอาการติดเทคโนโลยี
- มีปัญหาสุขภาพ เช่น ปวดตา ปวดหัว นอนไม่หลับ



- มีปัญหาด้านสังคม เช่น ขาดปฏิสัมพันธ์กับผู้อื่น มีปัญหาในความสัมพันธ์
- มีปัญหาด้านการเงิน เช่น ใช้จ่ายมากเกินไป

ดังนั้น การที่เราจะใช้เทคโนโลยี เครื่องมือ และสื่อดิจิทัลอย่างเหมาะสม
ไม่ส่งผลเสียจนทำลายสมดุลระหว่างชีวิตจริงและออนไลน์ จำเป็นต้องมี
การจัดการในหลากหลายด้าน แบ่งออกเป็น 3 กลุ่มใหญ่ ๆ ประกอบ
ด้วย

1

การดูแลสุขภาพบนโลกดิจิทัล (Digital Health)

ปกป้องสุขภาพกายและสุขภาพจิตในการใช้งานโลกดิจิทัล



2

การบริหารจัดการเวลาหน้าจอ (Screen Time Management)

จัดสรรเวลาในการใช้งานอุปกรณ์และสื่อดิจิทัลได้อย่างสมดุล



3

การมีส่วนร่วมอย่างสร้างสรรค์ในชุมชนดิจิทัล

ร่วมเสริมสร้างชุมชนดิจิทัลที่ดี และหลีกเลี่ยงผลกระทบเชิงลบ



การดูแลสุขภาพ บนโลกดิจิทัล (Digital Health)



เทคโนโลยีสามารถส่งผลกระทบต่อสุขภาพกายและสุขภาพจิตของเรา โดยหากเราใช้งานอย่างไม่สมดุล ย่อมส่งผลกระทบต่อสุขภาพทุกด้าน ดังนั้น การรักษาสุขภาพดิจิทัลที่ดีจึงมีความสำคัญ เพื่อให้เราสามารถใช้ประโยชน์จากเทคโนโลยีได้อย่างเต็มที่โดยไม่กระทบต่อสุขภาพของเรา

สุขภาพดิจิทัล (Digital Health) คือ การดูแลสุขภาพและความเป็นอยู่ที่ดี ในยุคดิจิทัล โดยมุ่งเน้นการใช้เทคโนโลยีอย่างเหมาะสมและสมดุล เพื่อส่งเสริมสุขภาพ ทั้งทางร่างกาย จิตใจ และการดำเนินชีวิตโดยรวม

การดูแลสุขภาพบนโลกดิจิทัล แบ่งเป็น 2 ด้าน คือ การดูแลสุขภาพกาย และการดูแลสุขภาพจิต

สุขภาพกาย (Physical Health)

ในการใช้งานดิจิทัลไม่ว่าผ่านอุปกรณ์ในรูปแบบใด ล้วนเกี่ยวโยงกับการใช้งานร่างกายแบบทั้งสิ้น ดังนั้น การใช้งานที่ผิดวิธีหรือมากเกินไป จะส่งผลโดยตรงต่อร่างกายอย่างหลีกเลี่ยงไม่ได้

1.1. ดวงตา



การมองภาพจากหน้าจออย่างไม่เหมาะสม อาจส่งผลให้มีอาการตาแห้ง แสบตา ปวดตา ตาพร่ามัว และอาจส่งผลต่อการมองเห็นในระยะยาวได้

วิธีดูแลสุขภาพตา :

พักสายตาทุก 20 นาที

มองไปไกล 20 ฟุต

เป็นเวลา
20 วินาที



- ใช้หลัก 20-20-20 คือ พักสายตาเป็นประจำทุก 20 นาที โดยละสายตาจากหน้าจอและมองไปยังวัตถุที่อยู่ไกลออกไปประมาณ 20 ฟุต เป็นเวลา 20 วินาที
- ปรับความสว่างหน้าจอให้อยู่ในระดับที่เหมาะสม ไม่สว่างหรือมืดเกินไป
- ใช้แสงไฟที่เหมาะสมในขณะใช้งานหน้าจอ หลีกเลี่ยงการใช้หน้าจอในที่มืด
- ตรวจสุขภาพตา กับจักษุแพทย์เป็นประจำ

1.2. หู



โดยเฉพาะผู้ที่มักใช้หูฟัง การฟังเสียงในระดับที่ดังเกินไปเป็นเวลานานส่งผลกระทบต่อหู และอาจทำให้สูญเสียการได้ยิน

วิธีดูแลสุขภาพหู :

- ปรับระดับเสียงให้เหมาะสม ไม่ดังเกินไป
- จำกัดเวลาในการใช้หูฟัง
- หากรู้สึกว่าหูอื้อหรือมีเสียงดังในหู ควรหยุดใช้หูฟังและปรึกษาแพทย์



1.3 ร่างกาย

การจัดตำแหน่งร่างกายในอิริยาบถต่าง ๆ หรือการขยับท่าทางแบบผิดวิธีอาจส่งผลให้เกิดอาการปวดหลัง ปวดคอ ปวดไหล่ และปัญหากระดูกสันหลังได้

วิธีดูแลร่างกาย : ใช้หลักการยศาสตร์ (Ergonomics)

- นั่งในท่าที่ถูกต้อง ขณะใช้งานคอมพิวเตอร์ หรืออุปกรณ์อื่น ๆ โดยให้หลังตรง ศีรษะอยู่ในแนวเดียวกับลำตัว และเท้าราบกับพื้น
- ปรับความสูงของเก้าอี้และโต๊ะให้เหมาะสม เพื่อให้ข้อมืออยู่ในระดับเดียวกับแป้นพิมพ์ และข้อศอกงอเป็นมุม 90 องศา
- ใช้ที่พักข้อมือเพื่อลดแรงกดบนข้อมือ
- ลุกขึ้นยืนและเดินไปมาบ้างทุก ๆ ชั่วโมง เพื่อลดการนั่งเป็นเวลานาน

1.4 การนอนหลับ

นอกจากการใช้งานทางร่างกายแล้ว การใช้งานดิจิทัลที่ไม่สมดุล ยังส่งผลกระทบอีกด้านหนึ่ง นั่นคือ การนอนที่ไม่มีคุณภาพนอน หลับไม่สนิทหรือยิ่งกว่านั้น คือ การนอนไม่เพียงพอ หรือนอนไม่หลับ การนอนทำงานโหมคุณภาพยนตร์ โหมเสพเนื้อหาความบันเทิง อาจเป็นสาเหตุหลักของการนอนที่ไม่มีคุณภาพ

อีกหนึ่งปัจจัยสำคัญที่ส่งผลกระทบต่อการนอน คือการใช้งานหน้าจอ เพราะ “แสงสีฟ้า” จากหน้าจอจะมารบกวนการผลิตเมลาโทนิน ซึ่งเป็นฮอร์โมนที่ช่วยในการนอนหลับของร่างกาย

วิธีแก้ไข

- จำกัดเวลาการใช้งานหน้าจอ หยุดใช้งานหน้าจอต่อ ၅ อย่างน้อย 1 - 2 ชั่วโมงก่อนนอน
- สร้างสภาพแวดล้อมการนอนหลับที่เหมาะสม มีด สงบ และอุณหภูมิที่เหมาะสม
- หลีกเลี่ยงการดื่มเครื่องดื่มที่มีกาแฟอีนหรือแอลกอฮอล์ก่อนนอน

1.5 สุขภาพโดยรวม

การใช้งานดิจิทัล อาจทำให้หลงลืมการดูแลใส่ใจสุขภาพโดยรวม อีกทั้งโดยส่วนใหญ่เรามักใช้งานโดยนั่งอยู่กับที่ (และอาจมีน้ำหวาน หรือขนมติดมือติดโต๊ะไม่ขาด) จึงเลี้ยงไม่ได้ที่จะเกิด “สภาวะเนอญนิ่ง” และอาจนำมาซึ่งโรคภัยไข้เจ็บ โรคไม่ติดต่อเรื้อรัง อย่างโรคเบาหวาน โรคอ้วน โรคหัวใจและหลอดเลือด โรคทางระบบประสาท รวมถึงปัญหาสุขภาพอื่น ๆ ตามมาได้

วิธีแก้ไข

- ให้ความสำคัญกับการใช้ชีวิตอย่าง ขยับร่างกายลงขั้นยืน และเดินให้มากเท่าที่จะได้
- ดูแลอาหารการกิน หากจำเป็นต้องมีอาหารว่าง ควรเลือกอาหารที่ไม่ส่งผลเสียต่อสุขภาพ เครื่องดื่มควรเน้นน้ำเปล่า หรือเครื่องดื่มที่ไม่มีน้ำตาลมากเกินไป
- จัดสรรเวลาออกกำลังกาย อย่างน้อย 30 นาทีต่อวัน 5 วันต่อสัปดาห์ โดยมองหากิจกรรมที่คุณชอบทำ เช่น เดิน วิ่ง ว่ายน้ำ หรือเล่นกีฬา
- ใช้เทคโนโลยีเพื่อช่วยติดตามและสร้างแรงบันดาลใจในการทำกิจกรรม หรือออกกำลังกาย เช่น แอปพลิเคชันนับก้าว สมาร์ตวอตช์ เป็นต้น



รู้จักหลัก

"การยศาสตร์" หรือ Ergonomics เคล็ดลับป้องกันผลกระทบต่อสุขภาพ

การยศาสตร์ (Ergonomics) คือ

วิทยาการเพื่อการทำงาน โดยใช้วิทยาศาสตร์ชื่อมโยงสัมพันธ์กับเนื้องาน บุคลากร สภาพแวดล้อม เพื่อออกแบบลักษณะของการทำงานให้มีประสิทธิภาพ ลดความเสี่ยง ผลกระทบต่อสุขภาพหรืออันตรายจากอุบัติเหตุ

- 1 ไม่ให้อาหารสายตา**
ใช้ร่างกายเป็นมาตรฐาน เมื่อร่างกายเริ่มมีอาการผิดปกติ ก็ควรหยุดพักจากการใช้งานก่อน
- 2 กฎ 20-20-20**
พักสายตาเป็นประจำทุก 20 นาที โดยละสายตาจากหน้าจอ และมองไปยังวัตถุ ที่อยู่ไกลออกไปประมาณ 20 พุต เป็นเวลา 20 วินาที
- 3 นั่งถูกต้อง**
ระหว่างที่อยู่หน้าจอควรจัดโต๊ะเก้าอี้ ให้นั่งอยู่ในท่าที่ถูกต้อง ไม่สร้างการบาดเจ็บต่อร่างกาย ปรับแสงหน้าจอให้อยู่ในระดับพอดี
- 4 ตั้งเป้าหมายการใช้งาน**
ตั้งเป้าหมายก่อนการใช้งาน หน้าจอทุกครั้ง และควรจำกัดเวลาการอยู่หน้าจอ
- 5 กำกิจกรรมอื่นบ้าง**
หากิจกรรมอย่างอื่นทำ ที่ไม่ต้องอยู่หน้าจอ ตลอดเวลา เช่น ออกกำลังกายอย่างน้อย 30 นาทีต่อวัน หรือออกไปท่องเที่ยว
- 6 พักผ่อนให้เพียงพอ**
รับประทานอาหารที่มีประโยชน์ นอนหลับพักผ่อนให้เพียงพอ อย่างน้อย 6 - 8 ชั่วโมงต่อคืน



สุขภาพจิต (Mental Health)

ในการใช้งานดิจิทัลนอกจากร่างกายที่มีปฏิสัมพันธ์กับอุปกรณ์ต่าง ๆ แล้ว ในขณะเดียวกันจิตใจและความรู้สึกนึกคิด ก็มีส่วนปฏิสัมพันธ์โดยตรงกับเนื้อหา ข้อมูลข่าวสาร และการตอบสนองต่อเหตุการณ์ทางดิจิทัลที่เกิดขึ้นด้วย

2.1 จัดการอารมณ์ และความรู้สึก

การสเปนเนื้อหา ข่าวสาร หรือพับเจอเหตุการณ์ที่มีความรุนแรง สะเทือนอารมณ์ และความรู้สึกก็อาจส่งผลทำให้เกิดความเครียด ความวิตกกังวล จนกล้ายเป็นโรคซึมเศร้าได้

วิธีแก้ไข

- จำกัดการรับข่าวสารและข้อมูลที่มากเกินไป เลือกติดตามข่าวสารจากแหล่งที่เชื่อถือได้ และจำกัดเวลาในการสเปนข่าวสาร
- การหมั่นฝึกสติและสมาธิ ช่วยให้เรามีสติอยู่กับปัจจุบัน และลดความฟุ้งซ่านในจิตใจได้
- หากิจกรรมที่ช่วยผ่อนคลายความเครียดทำ เช่น การฟังเพลง การอ่านหนังสือ การออกกำลังกาย หรือการทำกิจกรรมที่ชอบ
- พูดคุยกับเพื่อนหรือคนในครอบครัว แบ่งปันความรู้สึก กับคนใกล้ชิด จะช่วยลดความเครียด และความวิตกกังวลได้



2.2 ใส่ใจความสัมพันธ์กับคุณค่า

การใช้เวลา กับ เนื้อหา และ เทคโนโลยีมากเกินไป จะ ละ เลย ความ สัมพันธ์ กับ คน รอบ ข้าง อาจ ทำ ให้ รู้สึก โดด เดี่ยว และ มี ปัญหา ใน การ ปฏิสัมพันธ์ กับ คน จริง ๆ ได้

วิธีแก้ไข

- จัดสรรเวลา พบรูป คุยกับเพื่อน และ ครอบครัว เป็นประจำ การ มี ปฏิสัมพันธ์ กับ คน รอบ ข้าง จะ ช่วย ให้ เรา ไม่ รู้สึก โดด เดี่ยว
- เข้าร่วม กิจกรรม ทาง สังคม การ เข้าร่วม กิจกรรม ช่วย ให้ เรา ได้ พบรูป คุณ ใหม่ ๆ และ สร้าง ความ สัมพันธ์ ที่ ดี ต่อกัน ได้
- ใช้ เทคโนโลยี เพื่อ เชื่อมต่อ กับ คน ที่ เรายัง รัก การ ติดต่อ สื่อสาร กับ คน ที่ เรายัง รัก จะ ช่วย ให้ เรา รู้สึก ใกล้ชิด และ ได้ รับ การ สนับสนุน อุ่น ห่วง ใจ
- หลีกเลี่ยง การ เปรียบเทียบ ตัว เอง กับ ผู้ อื่น บน โซเชียล มีเดีย เพราะ อาจ ทำ ให้ เกิด ความ รู้สึก ไม่ พอดี ใน ตน เอง และ ลด ทอน ความ มั่นใจ



2.3 รู้กันพฤติกรรมการใช้เทคโนโลยี

การใช้เทคโนโลยีมากเกินไป อาจทำให้เกิดพฤติกรรมที่ส่งผลเสียต่อจิตใจ ลุกลามไปจนถึงการเสพติด หรือก่อให้เกิดภาวะซึมเศร้า ซึ่งไม่จำกัดอยู่แค่ในโลกดิจิทัล แต่แสดงผลในโลกความเป็นจริง

วิธีแก้ไข

- หมั่นสังเกตความผิดปกติทางจิตใจและพฤติกรรมของตนเอง รู้เท่าทัน ความรู้สึกนึกคิด ไม่ปล่อยให้สิ่งหวังกับตนเอง เพียงเพราะสิ่งที่พึ่งในโลกดิจิทัล
- ศึกษาข้อมูลเกี่ยวกับสุขภาพจิตจากแหล่งที่น่าเชื่อถือ เพื่อให้มีความรู้ ความเข้าใจเกี่ยวกับสุขภาพจิต และวิธีการดูแลตนเอง
- ใช้อ�플ิเคชัน หรือเครื่องมือออนไลน์ ที่ช่วยในการดูแลสุขภาพจิต เช่น แบบทดสอบสุขภาพจิต เป็นต้น
- หากสงสัยว่ามีปัญหาสุขภาพจิต ควรปรึกษาผู้เชี่ยวชาญ นักจิตวิทยา หรือจิตแพทย์ เพื่อเข้ารับการช่วยเหลือ หรือคำแนะนำในการจัดการ ปัญหาสุขภาพจิตได้อย่างมีประสิทธิภาพ



แนวทางป้องกันสุขภาพจิต จากผลกระทบด้านลบ

มีวิธีง่าย ๆ ดังต่อไปนี้



1 กำหนดระยะเวลาที่ใช้ในการเสพเนื้อหา

แบ่งเวลาที่ใช้เสพเนื้อหา เวลาพักผ่อนอย่างเหมาะสม เพื่อให้มี
แทรกแซงชีวิตประจำวัน



2 เลือกเนื้อหาที่ดีต่อสุขภาพจิต

เลือกเนื้อหาที่เชื่อถือได้ สร้างสรรค์ ให้ความบันเทิง และสร้าง
ประสบการณ์ที่ดีต่อตนเอง



3 ติดต่อกับสังคม

การติดต่อสังคมในโลกจริงจะช่วยลดความเหงา และเสริม
สุขภาพจิตที่ดีได้



4 หมั่นสังเกตตัวเอง

ว่ามีอาการ Digital Fatigue หรือไม่



5 ฝึกทักษะทางอารมณ์

ฝึกจัดการกับอารมณ์ของตนเอง เช่น การคิดบวก ผ่อนคลาย
ความเครียด ความโกรธ



TIP

Digital Fatigue

หรือ “การเหนื่อยล้าจากการใช้งานดิจิทัล”

คือ ภาวะที่เกิดขึ้นเมื่อเราสึกเหนื่อยหรือล้าจากการใช้งาน และการเชื่อมต่อกับเทคโนโลยีดิจิทัลอย่างต่อเนื่องหรือในปริมาณมาก โดยมักเกิดขึ้นเมื่อมีการใช้งานอุปกรณ์ดิจิทัล โปรแกรมคอมพิวเตอร์ และแพลตฟอร์มออนไลน์เป็นเวลานาน ๆ โดยไม่มีการพักผ่อน หรือการเปลี่ยนแปลงกิจวัตรประจำวัน

อาการ Digital Fatigue

คือ มักสึกเหนื่อยล้า มีความสับสน หรือไม่พร้อมที่จะดำเนินกิจวัตรประจำวันต่อไป เพราะการเหนื่อยจากการใช้งานดิจิทัลอาจมีผลกระทบทางกาย และจิตใจ เช่น ปวดตา ปวดหลัง ภาวะเครียด หรือภาวะซึมเศร้า

การดูแลและรักษา Digital Fatigue

ควรมีการจัดการเวลาที่ใช้ในโลกดิจิทัล เปลี่ยนแปลงกิจวัตรประจำวัน ให้ความสำคัญกับการดูแลสุขภาพจิต การใช้เทคโนโลยีอย่างมีสติ และมีความสมดุล จะสามารถช่วยลดความเหนื่อยล้าที่เกิดขึ้นจากการใช้งานดิจิทัลได้



การบริหารจัดการเวลาบนโลกดิจิทัล



การใช้เวลาหน้าจอ (Screen Time) คืออะไร ?

คือ คำที่ใช้เรียกกิจกรรมต่าง ๆ บนหน้าจอดิจิทัล โดยการใช้เวลาหน้าจอเกี่ยวข้องกับกิจกรรมหลายประเภท ดังนี้



- มีการโต้ตอบ เช่น การเล่นเกม การสื่อสารสนทนา



- ไม่มีการโต้ตอบ เช่น การนั่ง หรือนอนดูโทรทัศน์ หรือรายการในช่อง Streaming

การบริหารจัดการเวลาหน้าจอ



การบริหารจัดการเวลาหน้าจอ คือ ทักษะในการรู้จักควบคุมตนเอง และสามารถแบ่งเวลา ในการใช้งานอุปกรณ์เทคโนโลยี รวมถึง การเล่นเกมออนไลน์ และโซเชียลมีเดียได้อย่างมีประสิทธิภาพ รู้จักการสร้างสมดุล ระหว่างการใช้เวลาหน้าจอและกิจกรรมที่ต้องทำในชีวิตประจำวัน โดยไม่กระทบต่อสุขภาพตนเอง และความสัมพันธ์กับคนรอบข้าง



TIP



การใช้เวลาหน้าจอดิจิทัล ที่เหมาะสมกับแต่ละช่วงวัย

องค์การอนามัยโลก (WHO) แนะนำว่า

1 เด็กอายุต่ำกว่า 2 ปี



ควรหลีกเลี่ยงการใช้หน้าจอ

2 เด็กอายุ 2-5 ปี



ควรใช้เวลาไม่เกิน 1 ชั่วโมง
ต่อวัน และควรดูเฉพาะ
สิ่งที่ส่งเสริมพัฒนาการ
ทางด้านการศึกษา

3 เด็กอายุ 5 ปีขึ้นไป



ไม่ควรเกิน 2 ชั่วโมงต่อวัน
และไม่เกิน 3 ชั่วโมงต่อวัน
ในช่วงสุดสัปดาห์

4 ผู้ใหญ่



ควรเฉลี่ยแล้วไม่เกิน
วันละ 2 ชั่วโมง
ซึ่งจะถือว่าเป็นเวลาที่
ไม่ก่อให้เกิดอันตรายต่อสุขภาพ



ตั้นเหตุแห่งอาการเสพติดหน้าจอ



หรือ Screen Addiction

หากเราดำเนินชีวิตโดยใช้เวลาอยู่กับหน้าจอมากเกินไป ไม่ว่าจะเป็น หน้าจอโทรศัพท์ จอมือถือ คอมพิวเตอร์ หรือ Tablet หรือจอมือถือ อาจทำให้เรามีอาการเสพติดหน้าจอ หรือ Screen Addiction

ภาวะติดจอ (Screen Addiction)

หรืออาจเรียกว่า “ติดเทคโนโลยี” “ติดดิจิทัล” หรือ “ติดอินเทอร์เน็ต” หมายถึง ภาวะที่มีการใช้อุปกรณ์อิเล็กทรอนิกส์มากเกินไป จนส่งผลต่อการใช้ชีวิตประจำวัน

อาการที่บ่งบอกว่ากำลังเสพติดการใช้หน้าจอ

- 1) รู้สึกหงุดหงิดกระวนกระวาย เมื่อไม่ได้ใช้สื่อออนไลน์
- 2) ให้เวลา กับสื่อออนไลน์มากเกินไป จนละเลยกิจกรรมอื่น
- 3) ขาดสมาธิในการเรียนหรือการทำงาน
- 4) มีปัญหาด้านการนอนหลับ
- 5) มีภาวะซึมเศร้า วิตกกังวล ก้าวร้าว

ผลกระทบจากการเสพติดหน้าจอ ผลกระทบต่อร่างกาย มีดังนี้

01



ปัญหาด้านสายตา

ทำให้มีอาการตาแห้ง ตาล้า ปวดตา ตาพร่ามัว และอาจนำไปสู่โรคตาเสื่อมได้

02



ปัญหาด้านกล้ามเนื้อและกระดูก

การก้มหน้าจ้องหน้าจอเป็นเวลานาน อาจทำให้ปวดกล้ามเนื้อ แขนเกร็งตัว และอาจนำไปสู่ปัญหากระดูกสันหลังเสื่อมได้

03



ปัญหาด้านน้ำหนัก

การนั่งเป็นเวลานานอาจทำให้ร่างกายไม่เคลื่อนไหว แคมบากคนยังมีข้อหวานและเครื่องดื่มผสมน้ำตาลไม่ขาดมือ ส่งผลให้น้ำหนักเพิ่มขึ้นและเสี่ยงต่อโรคอ้วน โรคเบาหวาน และโรคหัวใจ

04



ปัญหาด้านนอนหลับ

แสงสีฟ้าจากหน้าจอสามารถ擾กกระบวนการหลัง梢ริโน เมลาโนนิน ที่เป็นสารซึ่งช่วยในการนอนหลับ ทำให้นอนหลับยากหรือนอนไม่หลับ

ผลกระทบจากการเสพติดหน้าจอ

ผลกระทบต่อการดำเนินชีวิต

01



ปัญหาด้านความสัมพันธ์

การใช้เวลา กับหน้าจอมากเกินไปอาจทำให้เราลดลง
ความสัมพันธ์กับคนรอบข้าง ขาดปฏิสัมพันธ์กับผู้อื่น
และอาจนำไปสู่ปัญหาทางอารมณ์ เช่น ภาวะซึมเศร้า^๑
และปัญหาด้านความสัมพันธ์

02



ปัญหาด้านการทำงาน

การใช้เวลา กับหน้าจอที่ไม่ใช่การทำงานมากเกินไป
อาจทำให้เราทำงานไม่มีประสิทธิภาพ ความรับผิดชอบ
ลดน้อยลง และอาจพลาดโอกาสในการทำงานได้

03



ปัญหาด้านการศึกษา

การใช้เวลา กับหน้าจอมากเกินไปอาจทำให้เราเสียสมาธิ
梧 แวงง่าย เรียนไม่เข้าใจ และอาจส่งผลต่อผลการ
เรียนได้

04



ปัญหาด้านการเงิน

การใช้เวลา กับหน้าจอ หรือโหลดออนไลน์ที่มีสินค้าอยู่
มากมาย ทำให้เราใช้จ่ายมากเกินไป เพราะซื้อสินค้า^๒
ได้ง่าย และหากเราไม่ดูแลสุขภาพ อาจจำเป็นต้องนำ
เงินที่หาได้ไปเป็นค่ารักษาพยาบาล



ห้ามใจจากจวไม่ได้

เรามีเครื่องมือง่าย ๆ มาช่วยจัดการได้นะ

เครื่องมือหรือเทคโนโลยี ที่ช่วยในการจัดสรรเวลาในการใช้เทคโนโลยี ดิจิทัล เช่น

1 To-Do List Apps

การใช้แอปพลิเคชันที่ช่วยจัดทำรายการสิ่งที่ต้องทำ (To-Do List) เป็นวิธีที่ดีในการจัดการเวลา ช่วยให้สามารถลิสต์งานที่ต้องทำ กำหนดเวลาและติดตามความคืบหน้าได้อย่างง่ายดาย เช่น Todoist, Microsoft, To-Do, Any.do เป็นต้น

2 Pomodoro Technique เทคนิค Pomodoro

เป็นวิธีที่มีประสิทธิภาพในการจัดการเวลาและเพิ่มความสนับสนุนในการทำงาน โดยทำงานในช่วงเวลาสั้น ๆ ประมาณ 25 นาที แล้วพักผ่อนเป็นช่วงสั้น ๆ ประมาณ 5 นาที การใช้แอปพลิเคชัน Pomodoro Timer ช่วยให้เราสามารถติดตามเวลาทำงานและพักผ่อนได้อย่างมีระเบียบ

3 Calendar Apps

การใช้แอปพลิเคชันปฏิทินช่วยในการจัดการกิจกรรมและกำหนดการ เช่น Google Calendar, Microsoft Outlook, Apple Calendar ในการจัดกิจกรรมทั้งระยะสั้นและระยะยาว

4 Digital Note-Taking Tools

การใช้เครื่องมือบันทึกข้อมูลช่วยในการจัดสรรเวลาเดียวกับข้อมูล เช่น Microsoft OneNote, Evernote หรือ Notion เป็นเครื่องมือช่วยในการจัดเก็บข้อมูล บันทึกความคิด และแบ่งปันไฟล์ ที่สามารถเข้าถึงได้ทุกที่ทุกเวลา

5 Focus Apps

แอปพลิเคชันที่ช่วยในการรักษาความมีสมาธิ และไม่ทำให้เสียเวลา เช่น Forest ที่ให้คุณปลูกต้นไม้ขณะที่คุณทำงานและต้องปอกป่องต้นไม้จนกว่าจะสำเร็จงาน

6 Digital Wellbeing Features

ระบบปฏิบัติการมือถือบางตัว มีคุณลักษณะส่งเสริมการใช้งานเพื่อสุขภาพ เช่น Digital Wellbeing ใน Android หรือ Screen Time ใน iOS ช่วยในการติดตามเวลาที่ใช้กับแอปพลิเคชันแต่ละตัว และตั้งค่าการจำกัดเวลาการใช้งานได้

การใช้งานเครื่องมือหรือเทคโนโลยีที่ช่วยในการจัดสรรเวลาในการใช้เทคโนโลยีดิจิทัล สามารถทำได้ดังนี้

เลือกเครื่องมือหรือเทคโนโลยีที่เหมาะสม

- ตามความต้องการ พิจารณาจากฟังก์ชันการใช้งาน และคุณสมบัติต่าง ๆ ของเครื่องมือหรือเทคโนโลยี

กำหนดการตั้งค่าให้เหมาะสมกับตนเอง

- เช่น กำหนดเวลาการใช้งาน บล็อกเว็บไซต์ หรือ แอปพลิเคชันที่ต้องการจำกัดการใช้งาน

ติดตามการใช้งานอย่างสม่ำเสมอ

- เพื่อให้มองเห็นภาพรวมของการใช้งาน และปรับเปลี่ยนพฤติกรรมได้

สุขภาพจิตกับการเสพติดเนื้อหา



นอกจากบางคนจะเป็นภาวะเสพติดจอแล้ว ก็อาจจะมีอาการที่เรียกว่า การเสพติดเนื้อหา

การเสพติดเนื้อหา (Content Addiction)

เป็นภาวะติดการเสพข้อมูล หรือเนื้อหานิสัยดิจิทัล เช่น โซเชียลมีเดีย เกมออนไลน์ และวิดีโอ

อาการของการเสพติดเนื้อหา

- ไม่สามารถควบคุมตัวเองได้เมื่อเห็นเนื้อหาที่สนใจ
- ใช้เวลาไปกับเนื้อหามากเกินไปจนกระทบต่อการเรียน การงาน หรือ ความสัมพันธ์กับคนรอบข้าง
- รู้สึกหงุดหงิดหรือรู้สึกรำคาญรำคาญเมื่อไม่ได้เสพเนื้อหา

สาเหตุของการเสพติดเนื้อหา มีดังนี้

- ปัจจัยทางชีวภาพ พบร่วมกับความต้องการของผู้เสพติดเนื้อหา มักมีสารโดปามีน ในระดับต่ำ ซึ่งสารโดปามีนนี้ ทำหน้าที่ควบคุมอารมณ์ การเรียนรู้ และการเคลื่อนไหว
- ปัจจัยทางจิตวิทยา ผู้เสพติดเนื้อหามักมีแนวโน้มที่จะรู้สึกโดยเดียว เหงา หรือขาดความมั่นใจในตัวเอง
- ปัจจัยทางสังคม สังคมในปัจจุบันให้ความสำคัญกับเทคโนโลยีเป็นอย่างมาก ผู้คนมักใช้เวลาส่วนใหญ่ไปกับการใช้อุปกรณ์ดิจิทัล ซึ่งอาจกระตุ้นให้เกิดพฤติกรรมเสพติดเนื้อหาได้

**TIP**

สารโดปามีน (Dopamine)

เป็นสารสื่อประสาทที่มีบทบาทสำคัญเรื่องอารมณ์ และความรู้สึก มักถูกเรียกว่าเป็นสาร "รู้สึกดี" เพราะถูกปล่อยออกมาเพื่อตอบสนองต่อประสบการณ์ที่น่าพึงพอใจ และสามารถช่วยยกระดับอารมณ์ได้

- หากสารโดปามีนถูกหลั่งจากสมองสูงขึ้น อาจส่งผลให้มีความสุข รู้สึกรัก พึงพอใจ ทำให้มีความตื่นตัวกระฉับกระเฉง มีสมาธิจดจ่อ และไวต่อสิ่งกระตุ้นรอบตัว
- แต่ถ้าสารโดปามีนต่ำลง หรือหยุดทำงาน จะส่งผลให้เกิดอารมณ์หดหู่ เหงา และซึมเศร้า



การเสพติดเนื้อหา



มักจะส่งผลให้เกิดผลเสียต่อสุขภาพจิต

① ด้านอารมณ์

การติดตามเนื้อหา หรือข่าวสารที่มีความเครียดสูง นำเสนอด้วยความไม่เข้มงวดในชีวิต สามารถทำให้เกิดความเครียดที่ไม่จำเป็น มีความวิตกกังวล หรืออาการซึมเศร้าได้

② ด้านความสัมพันธ์

การที่เราเสพติดเนื้อหาและใช้งานอินเทอร์เน็ตมาก ๆ จะละเลยคนรอบข้าง และในชีวิตริงกลับทำอะไรคนเดียว เมื่อเกิดปัญหาขึ้นเราอาจจะไม่มีคนให้ปรึกษา ไม่ไว้ใจใคร รู้สึกโดดเดี่ยว

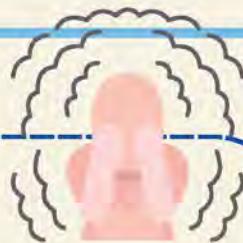
③ ด้านพฤติกรรม

การใช้เวลาในการเสพติดเนื้อหามากเกินไป อาจทำให้ขาดสมดุลในชีวิต ระหว่างการทำงาน การพักผ่อน และสังคม มีผลต่อสุขภาพจิตที่ดี

นอกจากนี้ อาจนำไปสู่ปัญหาสุขภาพจิตอื่น ๆ เช่น โรคย้ำคิดย้ำทำ (OCD) โรควิตกกังวลทางสังคม (SAD) และโรคบุคลิกภาพแบบก้ากึ่ง (BPD) หากพบว่าตัวเองมีปัญหารื่องการเสพติดเนื้อหา ให้ลองปรึกษาผู้เชี่ยวชาญเพื่อขอคำแนะนำ



TIP



โรคย้ำคิดย้ำทำ

(OCD หรือย่อมาจาก Obsessive Compulsive Disorder) เป็นโรคทางจิตเวชชนิดหนึ่ง ที่ผู้ป่วยจะมีความกังวลหรือความไม่มั่นใจต่อสิ่งใดสิ่งหนึ่ง จึงพยายามแก้ไขด้วยการทำกิจกรรมบางอย่างซ้ำไปซ้ำมา

โรควิตกกังวลทางสังคม

(SAD หรือย่อมาจาก Social Anxiety Disorder)

การที่ผู้ป่วยมีอาการประหม่า รู้สึกไม่สบายใจ อึดอัด กังวลใจ เมื่อยู่ในสถานการณ์ที่อาจมีผู้อื่นสังเกตจ้องมองตนเองอยู่

โรคบุคลิกภาพแบบก้าว

(BPD หรือย่อมาจาก Borderline Personality Disorder)

เป็นความผิดปกติทางจิต ที่ส่งผลต่อความคิดและความรู้สึกที่ผู้ป่วยมีต่อตนเองและผู้อื่น ผู้ป่วยอาจมีอารมณ์ซึ้น ๆ ลง ๆ อารมณ์รุนแรง หุนหันพลันแล่น มีความคิดและนิสัยไม่คงที่ ซึ่งส่งผลให้มีปัญหาในการรักษาความสัมพันธ์กับผู้อื่น และการใช้ชีวิตประจำวัน



TIP

ติดจนตัวต้านสังคม

คนที่ติดจนมากเกินไป อาจมีพฤติกรรมต่อต้านสังคม อันเนื่องมาจากการเสพเนื้อหาที่มีความรุนแรง หรือขัดแย้งอย่างต่อเนื่อง ทำให้มีความเห็นที่สุดโต่ง มีการแสดงออกที่ก้าวร้าว ด่าหอผู้อื่นโดยไม่รู้ตัว

- มีการศึกษาพบผู้ที่มีระดับการติดหน้าจอสูง รวมทั้งการได้รับเนื้อหาที่รุนแรงบนหน้าจอบ่อยครั้ง มีแนวโน้มที่จะแสดงพฤติกรรมก้าวร้าวมากขึ้น
- การใช้เวลาบนหน้าจอมากเกินไป อาจเพิ่มโอกาสการถูกกลั่นแกล้งทางไซเบอร์ ส่งเสริมความคิดที่ไม่เหมาะสม ทำให้รู้สึกว่าพฤติกรรมที่เป็นอันตรายเป็นเรื่องปกติ รวมทั้งความก้าวร้าวต่อผู้อื่น
- การใช้หน้าจอมากเกินไป อาจขัดขวางการพัฒนาความเห็นอกเห็นใจ และทักษะการควบคุมอารมณ์ ทำให้บุคคลไม่ค่อยไวต่อความรู้สึกของผู้อื่น และมีแนวโน้มที่จะมีพฤติกรรมที่ไม่เหมาะสม





ลักษณะเนื้อหาที่เราควรพิจารณา เพื่อป้องกันการเผยแพร่เนื้อหาที่ไม่เหมาะสม

- 1 มีความถูกต้องแม่นยำ ไม่บิดเบือนหรือจงใจใส่ข้อมูลเท็จ
- 2 มีความเป็นปัจจุบัน ทันสมัยและทันต่อเหตุการณ์
- 3 กระชับ ชัดเจน เข้าใจง่าย และตรงประเด็น
- 4 มีความเหมาะสมกับกลุ่มเป้าหมายที่ตั้งใจจะสื่อสาร
- 5 สร้างสรรค์ น่าสนใจและเป็นประโยชน์ต่อผู้อื่น
- 6 ไม่มีเนื้อหาที่ก่อให้เกิดความขัดแย้ง ความรุนแรง และอคติ
- 7 หลีกเลี่ยงเนื้อหาที่ไม่เหมาะสมกับศีลธรรม จริยธรรม
- 8 ไม่มีเนื้อหาละเมิดลิขสิทธิ์
- 9 ไม่มีภาพหรือเนื้อหาเชิงล้อเลียน ขบขัน หรือภาพแอบถ่ายโดยไม่ได้รับอนุญาต

การจัดการ และตั้งค่าการเข้าถึงเนื้อหาบนแพลตฟอร์มต่าง ๆ เพื่อป้องกันการเสพติดเนื้อหา

ตั้งค่าการกรองเนื้อหาแพลตฟอร์มต่าง ๆ

ตั้งค่าให้กรองเนื้อหาตามคำหลักที่เราต้องการบนโซเชียลอย่าง แพลตฟอร์ม X (Twitter) ตรงหัวข้อ ความเป็นส่วนตัว และความปลอดภัย ด้วยการกำหนดคำเพื่อซ่อนและบล็อกคำที่ต้องการ เช่น ผู้ตัวตาย การทำร้ายร่างกาย ยาเสพติด



จำกัดระยะเวลาในอ่านหรือเข้าชมเนื้อหา

ของแอปพลิเคชันต่าง ๆ ด้วย Digital Well-being เช่น การตั้งค่าการจำกัดระยะเวลาในการรับชมเนื้อหาบน YouTube โดยเริ่มจากที่เรากำหนดเวลาไว้ว่าจะใช้ YouTube ต่อวัน กี่ชั่วโมง เมื่อทำการตั้งค่าแล้ว หากเราใช้เกินเวลาไปก่อน แอปฯ จะกลายเป็นสีเทา และขึ้นเตือนว่าเราใช้งานเกินเวลา

เลือกติดตาม

หรือเป็นเพื่อนกับคนที่ส่งเนื้อหาที่ดีและมีประโยชน์ ซึ่งจะช่วยให้เราได้รับเนื้อหาที่ดีและมีประโยชน์มากขึ้น

FOLLOW



หากจกรนอื่น ๆ กำ

แต่งการเสพเนื้อหา เช่น ออกกำลังกาย ทำงานอดิเรก

การมีส่วนร่วมอย่างสร้างสรรค์ ในชุมชนดิจิทัล



เทคโนโลยีดิจิทัลทำให้เราสามารถติดต่อสื่อสาร มีปฏิสัมพันธ์ เรียนรู้ แบ่งปันข้อมูลข่าวสารกันในสังคมได้อย่างหลากหลายมากยิ่งขึ้น ผ่านการมีส่วนร่วมในชุมชนดิจิทัล โดยใช้เครื่องมือและแพลตฟอร์มออนไลน์ต่าง ๆ อย่างไรก็ตาม การมีส่วนร่วมในชุมชนดิจิทัล ก็มีรูปแบบการใช้ที่ไม่สมดุล และส่งผลกระทบเชิงลบ เช่นเดียวกัน อาทิ

- 1** การใช้โซเชียลมีเดียที่มากเกินความจำเป็น ทั้งด้านเวลาหรือการเผยแพร่ข้อมูล
- 2** การเปิดรับหรือเผยแพร่ข้อมูลเท็จหรือบิดเบือน รวมถึงการเข้าร่วมกลุ่มปิดที่มีการตีกรอบขอบเขตความเชื่อเพียงด้านเดียว ซึ่งอาจนำไปสู่การปลูกปั้นปลุกระดม
- 3** การคุกคามทางออนไลน์ หรือ การถูกคุกคามทางออนไลน์ ผ่านช่องทางที่หลากหลาย
- 4** การเสียโอกาสทางสังคม จากการใช้งานที่ไม่เหมาะสม ซึ่งอาจขยายผลกระทบไปถึงขั้นการถูกดำเนินคดีตามกฎหมาย

หลังจากที่เราได้เข้าใจถึงเรื่องการดูแล และบริหารจัดการเพื่อสุขภาพกาย สุขภาพใจ ตลอดจนการใช้งานอุปกรณ์ดิจิทัลอย่างสมดุล และภาพรวม ขั้นต้นของการมีส่วนร่วมในชุมชนอย่างสมดุลกันแล้ว ในบทดังไปเราจะได้ เรียนรู้ลงลึกยิ่งขึ้น เกี่ยวกับการใช้งานเทคโนโลยีที่ส่งผลกระทบเชิงบวกต่อ สังคม ผ่านหัวข้อ “Civic Use of Technology” การใช้เทคโนโลยีเพื่อ สังคมและตนเอง”





ปัจจุบันการใช้งานสื่อทั้งหลาย
 มีเทคโนโลยีมาอย่างสมดุลคุณอนันต์
 ใช้ให้เหมาะสมอย่างสมดุลคุณอนันต์
 ควรจัดสรรเพื่อส่งเสริมชีวิตดี
 เริ่มตอนนี้สุขภาพการยศาสตร์
 อย่าพลังพลาดเสพเนื้อหาน่าบัดสี
 ควรจัดการหน้าจอไม่รอรี
 ร่วมกันเสริมสุขศรีสร้างชุมชน



ถ้าคุณเรียนผ่านด้านนี้
คุณจะมีส่วนช่วย
ทำให้โลกออนไลน์ดียิ่งขึ้น
และไม่เสี่ยงทำผิดกฎหมาย
ที่มีโทษสูงทั้งจำและปรับ

*การโพสต์ด่าบุคคลอื่น ประจานแบบระบุชื่อ-นามสกุล ลงรูป โดยมีลักษณะเป็นการเผยแพร่ข้อความอันเป็นการหมิ่นประมาทออกไปยังสาธารณะ เป็นความผิดอาญา ฐานหมิ่นประมาทผู้อื่นด้วยการโฆษณาตามประมวลกฎหมายอาญา มาตรา 326 และมาตรา 328 โทษจำคุกไม่เกิน 2 ปี และปรับไม่เกิน 2 แสนบาท

2.2

CIVIC USE OF TECHNOLOGY

วัตถุประสงค์

- ผู้เรียนสามารถเข้าใจถึงการใช้เทคโนโลยีในการตอบโต้ แสดงความคิดเห็นมีปฏิสัมพันธ์ ดิตตาม และสภาพดีเนื้อหาดิจิทัลที่มีผลกระทบต่อสุขภาพจิตของตนเองและผู้อื่นได้
- ผู้เรียนสามารถตระหนักรถที่เกิดจากการมีปฏิสัมพันธ์ โดยใช้เทคโนโลยีในโลกดิจิทัลที่อาจผลมีต่ออารมณ์ ความรู้สึก และความต้องการของตนเองและผู้อื่น
- ผู้เรียนสามารถ อธิบายผลของการเอาใจเขามาใส่ใจเราทางดิจิทัล (DIGITAL EMPATHY) ได้
- ผู้เรียนสามารถเข้าใจถึงการสร้างค่านิยมเชิงบวกต่อชุมชนและสังคม ผ่านเทคโนโลยีที่เหมาะสมได้
- ผู้เรียนสามารถเข้าใจถึงการนำเทคโนโลยีมาใช้เพื่อพัฒนาและยกระดับคุณภาพชีวิตได้
- ผู้เรียนสามารถเลือกใช้วิธีการค้นหาข้อมูล รวบรวม และจัดการข้อมูล ที่ต้องการจากสื่อดิจิทัล

การใช้เทคโนโลยีในโลกดิจิทัล เพื่อสังคม และtanweong

เทคโนโลยีช่วยให้เราติดต่อสื่อสาร และมีปฏิสัมพันธ์กับผู้คนหรือสังคมได้มากขึ้น โดยมีหลากหลายรูปแบบการใช้เทคโนโลยี ซึ่งสามารถแบ่งออกเป็น

1 การตอบโต้

เป็นรูปแบบพื้นฐานที่สุดในการใช้เทคโนโลยีเพื่อโต้ตอบกับผู้อื่น สามารถทำได้หลายช่องทาง เช่น อีเมล แชท โดยการตอบโต้ควรมีความสุภาพ หมายความว่า ไม่สร้างความขัดแย้ง

2 การแสดงความคิดเห็น

รูปแบบหนึ่งของการสื่อสารที่ช่วยให้ผู้อื่นได้รู้ถึงความคิด และความรู้สึกของเรา เช่น Comment ใต้โพสต์ เขียนบทความ รีวิวสินค้า โดยการแสดงความคิดเห็นที่ดีควรมีความสร้างสรรค์ เป็นประโยชน์ และไม่ใช้คำพูดที่รุนแรง หรือก้าวร้าว

3 การมีปฏิสัมพันธ์

รูปแบบของการโต้ตอบมีส่วนร่วมกับผู้อื่นอย่างจริงจัง เช่น การพูดคุย การเล่นเกม การแชร์ประสบการณ์ ซึ่งการมีปฏิสัมพันธ์ที่ดี ควรมีความสร้างสรรค์ สนุกสนาน และสร้างความสัมพันธ์ที่ดีกับผู้อื่น

4 การติดตาม

รูปแบบของการรับรู้ข้อมูลข่าวสารจากผู้อื่น เช่น การกดติดตามเพจ กดติดตามผู้ใช้ หรือสมัครสมาชิก เป็นต้น ซึ่งการติดตามที่ดีควรเลือกติดตามแหล่งข้อมูลที่น่าเชื่อถือ และควรมีวิจารณญาณในการรับข้อมูล

5 การสภาพดิด

รูปแบบการใช้เทคโนโลยีที่ส่งผลกระทบต่อชีวิตประจำวัน เช่น การใช้เวลาอยู่กับหน้าจอมากเกินไป ขาดการติดต่อกับผู้อื่น การสภาพดิดเทคโนโลยีเป็นปัญหาที่ควรได้รับการแก้ไข โดยควรจำกัดเวลาในการใช้เทคโนโลยี ทำกิจกรรมอื่น ๆ ทดแทน และปรึกษาผู้เชี่ยวชาญหากจำเป็น



การจัดการผลกระทบ จากการใช้งานเทคโนโลยีดิจิทัล

ผลกระทบ ทางบวก

การตอบโต้ แสดงความคิดเห็น มีปฏิสัมพันธ์ การติดตาม และสภาพดีเนื่องจากเทคโนโลยีดิจิทัล มีผลกระทบอย่างมีนัยสำคัญต่อทั้งบุคคลและสังคมที่เรารอยู่ในปัจจุบัน ดังนั้น จึงจำเป็นต้องเข้าใจผลกระทบด้านบวกและด้านลบที่อาจเกิดขึ้น ดังนี้

01



ทำให้เราได้รับข้อมูลข่าวสาร และประสบการณ์ใหม่ จากผู้อื่น ซึ่งอาจเป็นประโยชน์ต่อการเรียนรู้ และการพัฒนาตนเอง

02



ใกล้แค่ไหนก็เหมือนใกล้กัน เมื่อเทคโนโลยีทำให้การเชื่อมต่อกับผู้คน และสร้างปฏิสัมพันธ์ที่ดีได้ง่ายขึ้น สามารถพูดคุย สื่อสาร ทำกิจกรรมร่วมกันกับเพื่อน หรือสมาชิกในกลุ่มบนโลกดิจิทัลได้ แม้ว่าจะอยู่กันคนละจังหวัด หรือคนละประเทศก็ตาม

03



เทคโนโลยีช่วยให้เราแสดงความรัก ความยินดี ความห่วงใยได้ตลอดเวลา ผ่านทางรูปภาพ ข้อความ เสียง หรือคลิปวิดีโอ และยังช่วยให้สามารถเข้าไปสอบถาม เสนอทางออกในปัญหาของคนที่ต้องการ ได้ง่ายดายมากขึ้นด้วย

ผลกระทบ ทางลบ

01



ปัญหาสุขภาพกายและสุขภาพจิต อาจเกิดขึ้นได้จากการอยู่กับหน้าจอมากเกินไป

02



ปัญหาจากสื่อที่ส่งไปไม่ครบมิติ ตัวหนังสือไม่มีเสียง ตัวอักษรไม่สามารถสื่อถึงน้ำเสียงของเรารaได้ หากไม่ระวังก็อาจทำให้เกิดความเข้าใจผิดหรือรู้สึกไม่ดีได้

03



การตีความของแต่ละบุคคลต่างกัน ความขัดแย้งอาจเกิดขึ้นได้เพียงแค่กดไลก์ในเรื่องราวน่าเศร้า เพราะการเข้าใจผิดจากการตีความด้านลบ เมื่อเกิดความไม่พอใจก็อาจจะนำไปสู่คติ และปัญหาการกลั่นแกล้งทางออนไลน์ได้

04



บุนโลกออนไลน์ แทบทุกเรื่องเป็นเรื่องสาระณะ หากเราไม่ได้ตั้งค่าจำกัดความเป็นส่วนตัว ก็จะเหมือนเรายืนตากแดดกันอยู่ที่ริมถนน ไม่ว่าจะดีหรือร้าย คนที่อยู่รอบ ๆ ก็จะรับรู้ได้โดย ถึงแม้เขาจะทำเป็นไม่สนใจ แต่บางเรื่องก็ทำให้ตัวเรานั้นเกิดความอับอาย จนกลายเป็นตัวเรื่องความขัดแย้งให้เกิดไวมากขึ้น เรียกว่า "หน้าต่างมีหู ประทุมีตา" ของแท้

05



ไม่กล้าบอกออกไป เมื่อเราเห็นคนส่วนมากพูด หรือคอมเมนต์ ไปในทางเดียวกัน แต่เรามีความเห็นที่ตรงกันข้าม ก็อาจทำให้เราตัดสินใจเก็บความเห็น หรือปัญหาเหล่านั้น เอาไว้คุณเดียว เพราะคิดว่าคงไม่มีใครเห็นด้วยกับเรา

06



ได้รับข้อมูลข่าวสารที่ผิด อาจส่งผลเสียต่อการตัดสินใจ หรือการดำเนินชีวิต

แนวทางการใช้เทคโนโลยีอย่างเหมาะสม

เพื่อหลีกเลี่ยงผลกระทบด้านลบ สิ่งสำคัญคือต้องรู้จักใช้เทคโนโลยีอย่างเหมาะสม ดังนี้

1) สุภาพและมีมารยาทไว้ก่อน

การตอบโต้ หรือแสดงความคิดเห็นบนโลกดิจิทัล ควรหลีกเลี่ยงการใช้ถ้อยคำที่รุนแรง ไม่สุภาพ และล้าเส้นความเป็นส่วนตัว

2) ตระหนักว่าโลกดิจิทัลกว้างใหญ่ไร้ขีดจำกัด

ผู้คนที่เข้ามาอ่าน มาแสดงความเห็นนั้นมีความหลากหลาย ทั้งระดับความรู้ ทศนคติ และความเชื่อ ย่อมมีคนเห็นต่าง และเกิดความขัดแย้งได้อย่างเพียงด่วนดีใจหรือเคร้าใจมากจนเกินความจริง

3) อย่าให้ความคิดเห็นของเราตัดสินคนอื่น

ข้อความของเราอาจทำให้ผู้อื่นได้รับความเสียหายได้ ในบางครั้งความรู้หรือแนวคิดที่เราเชื่อมั่น อาจจะทำให้คนอื่นรู้สึกอึดอัด ไปจนถึงรู้สึกไม่ดีกับเราได้

เข้าอกเข้าใจกัน ผ่าน Digital Empathy

แม้การสื่อสารบนโลกดิจิทัล ยกที่จะถ่ายทอดและรับรู้อารมณ์ความรู้สึกระหว่างกัน แต่ไม่ได้แปลว่ามันไม่มีอยู่ และในทางตรงกันข้าม มันอาจถูกขยายหรือลดความรู้สึกได้ด้วยเช่นกัน ความดีใจถูกขยาย ความเจ็บปวดใจถูกขยาย จึงเป็นเหตุให้เราต้องใส่ใจกับอุปกรณ์มือที่สำคัญในโลกดิจิทัล สิ่งนี้เรียกว่า Digital Empathy



Digital Empathy

หรือ การเอาใจเขามาใส่ใจเราทางดิจิทัล

หรือบางท่านเรียกว่า "การร่วมรู้สึกทางดิจิทัล" ซึ่งเป็นทักษะที่สำคัญในยุคปัจจุบัน ซึ่งจะช่วยให้เราเข้าอกเข้าใจผู้อื่นได้มากยิ่งขึ้น และไม่พลาดพลั้ง จากการละเลยความรู้สึกของกันและกัน จากรายงาน DQ Global Standards Report ระบุว่า คนที่มี Digital Empathy จะมีลักษณะอย่างน้อย 3 ประการ

1

เข้าใจผลกระทบของการแสดงออก

ผ่านโลกออนไลน์ที่มีต่อผู้อื่น

โดยเฉพาะในด้านความรู้สึก และการส่งอิทธิพล
ต่อความคิดหรือพฤติกรรม



2

เคารพมนุษย์ และอารมณ์ที่หลากหลาย

เมื่อเข้าสู่การปฏิสัมพันธ์บนโลกออนไลน์



3

แสดงออกซึ่งความเห็นอกเห็นใจ

ผู้อื่นบนโลกออนไลน์

ทั้งด้านอารมณ์ ความจำเป็น ความต้องการ
ความกังวลใจ และความใส่ใจ



แนวทางการพัฒนาทักษะ Digital Empathy

1. เป็นนักฟังอย่างตั้งใจ

มองให้ลึกกว่าแค่ตัวอักษร อิโมจิ หรือสติกเกอร์ ที่ไม่สามารถเล่าเรื่อง และบริบทได้ทั้งหมด แต่ให้นึกถึงสิ่งที่อยู่เบื้องหลังการสื่อสารเหล่านั้น

2. เป็นนักมองต่างมุม

ฝึกให้เชี่ยวชาญการมองจากมุมของผู้อื่น โดยเฉพาะในโลกออนไลน์ที่กำแพงทางภูมิศาสตร์พังทลายลง

3. เป็นนักสื่อสารที่รอบคอบ

สารบันออนไลน์ ง่ายจะถูกตีความผิด ดังนั้น พึงหลีกเลี่ยงการเสียดสี ใช้อิโมจิอย่างระวัง และอ่านทวนซ้ำก่อนกด "ส่ง"

4. เป็นนักเชื่อในส่วนดี

เมื่อรู้สึกเป็นฝ่ายถูกกระทำ หรือเห็นอะไรที่ดูโง่ผาง ให้คิดไว้ก่อนว่าอีกฝ่ายนั้นมีเจตนาที่ดี รวมไปถึงช่วงเว翕 Ital ของการทะเลาะ เช่น การไม่กดอ่าน อ่านไม่ตอบ ตอบช้าไม่ทันใจนั้น คุณไม่มีทางรู้ว่าสถานการณ์ "โลกรจริง" ในขณะนั้นของอีกฝ่ายเป็นอย่างไร เพียงแค่เฝ้าดูจากจอมมองเห็นแค่โลกออนไลน์

5. เป็นนักการพูดความเห็นต่าง

แม้จะไม่เห็นด้วยกับเขา จงแสดงออกถึงท่าที่แห่งความรับรู้โดยเคารพ และให้เกียรติในสิทธิในการแสดงความคิดเห็น รวมทั้ง การรู้จักและเข้าใจ อารมณ์ของตัวเองในทุกขณะ

6. ระวังตกลร้าย มากไม่ข้า

“คุณยา แต่คนอื่นไม่จำเป็นต้องยา” โดยเฉพาะถ้ามุกนั้น ไม่ใช่แค่เป็ก แต่ยังอาจทำร้ายจิตใจหรือสร้างความแตกแยกได้

7. ระวังอุบัติเหตุทางดิจิทัล

“แมวพิมพ์” “แบบตหมด” “เน็ตหลุด” “ลีมตังเตือน” “ใส่ผิดวัน” ฯลฯ ล้วน มีโอกาสเกิดขึ้นได้เสมอ ในยุคที่มุขย์ต้องพึ่งพา “อุปกรณ์” ในการสื่อสาร ระหว่างกัน หลีกเลี่ยงการแสดงออกหรือสร้างความรู้สึกดันจากเฉพาะ นุ่มนองของตนเอง ไม่เพียงทำร้ายจิตใจ แต่ยังอาจถลายความสัมพันธ์อัน มีค่า

8. สะสมคลังคำสาหัสท่อนอารมณ์

ยิ่งเราสื่อสารกับคนหลากหลาย เรา>yิ่งต้องใส่ใจที่จะเข้าใจและไว้ต่อ คำสื่อความรู้สึกทั้งหลายเพื่อเราจะหยิบใช้ได้อย่างเหมาะสมทั้งในบทบาท ของผู้ฟังและผู้พูดไม่ต่างกับการเรียนรู้ภาษาใหม่ เมื่อคนที่เข้าใจทั้ง ภาษากลาง และภาษาถิ่น ก็จะยิ่งมีทักษะในการเข้าอกเข้าใจคนจำนวน มากขึ้น

เจอย่างนี้...รับมือย่างไร ?

เราลองมาดูกันดีกว่าว่า ถ้าเราต้องเจอกับสถานการณ์ที่กระทบต่อความรู้สึก และความต้องการจากเนื้อหาที่มีคนสื่อสาร หรือปฏิสัมพันธ์บนโลกดิจิทัล จะจัดการอย่างไร เพื่อให้ผู้รับสายใจ และผู้ให้รู้สึกดีกัน

กรณีที่ 01

คนใกล้ชิด หรือสนิทสนม ที่เคยหยอกล้อกัน โพสต์ข้อความ หรือภาพที่ส่อถึงความสิ้นหวัง หมดกำลังใจ

ไม่ควรทำ



โพสต์ หรือแสดงความคิดเห็นหยอกล้อให้รู้สึกสนใจ เนื่องจากตัวหนังสือไม่มีน้ำเสียงและสื่อความรู้สึกได้ลำบาก อาจจะตีความหมายที่จะสื่อสารผิดได้อีกทั้งการตอบโต้ของเรานอกจากจะประกายแก่เพื่อนเจ้าของโพสต์แล้ว เพื่อนของเพื่อนที่ติดตามก็เห็นด้วย แม้ว่าเพื่อนเราจะเข้าใจ แต่คนอื่นอาจไม่เข้าใจ และอาจมีการตอบโต้กันไปมา

ควรทำ



โพสต์ หรือแสดงความคิดเห็นอย่างจริงใจ และตรงไปตรงมา หากรู้สึกเป็นห่วง ให้บอกความรู้สึกไปตรง ๆ ตระหนักอยู่เสมอว่า เราไม่เพียงแค่สื่อสารกับคน ๆ นั้นเท่านั้น แต่ยังมีอีกหลายคนซึ่งเป็นเพื่อนของเขาระบุ อาจจะเป็นครรภ์ได้เห็นข้อความของเรา และตีความหมายไปต่าง ๆ นานา ตามประสบการณ์ของเขางง ระมัดระวัง ก่อนที่จะแสดงความคิดเห็นอะไรไป เพราะจากห่วงใยอาจกลายเป็นDRAM ได้

กรณีที่

02

น้องชายที่เรามองว่า ไม่ค่อยตั้งใจเรียน โพสต์ข้อความว่า
ทำงาน ไม่มีงานทำ และกำลังทำงานในภาวะเศรษฐกิจตกต่ำ

ไม่ควรทำ



โพสต์ หรือคอมเมนต์สั่งสอน หลายครั้งเมื่อเห็นภาพหรือข้อความลูกหลาน
ที่ไม่ได้ดั่งใจ อาจจะแสดงอารมณ์กรรช หงุดหงิด ฉุนเฉีย หรืออยากสั่ง
สอน แล้วโตตوبด้วยข้อความหรือสื่อที่ไม่เหมาะสม ในเชิงลดทอนกำลังใจ
หรือซ้ำเติม แต่ไม่ได้ประสงค์ร้าย และทำด้วยความเป็นห่วงด้วยซ้ำ แต่หาก
เคยทำอะไรผิดพลาดหรือไม่ใช่คนสมบูรณ์แบบกันทั้งนั้น

ควรทำ



โพสต์ หรือคอมเมนต์ให้กำลังใจและพร้อมสนับสนุน หรือให้คำแนะนำใน
ช่องทางส่วนตัว





การใช้เทคโนโลยีอย่างเหมาะสม เพื่อสร้างค่านิยมเชิงบวกต่อชุมชน และพัฒนาคุณภาพชีวิต



ค่านิยมเชิงบวกในการใช้เทคโนโลยีให้เหมาะสม

1) ความรับผิดชอบ

รับผิดชอบต่อการกระทำของตน ตระหนักถึงผลกระทบต่อผู้อื่น และสังคม

2) ความเคารพ

เคารพความแตกต่าง และวัฒนธรรมของผู้อื่น ไม่ใช้เทคโนโลยี เพื่อละเมิด หรือกลั่นแกล้งผู้อื่น

3) ความสามัคคี

ใช้เทคโนโลยีเพื่อเชื่อมโยงเข้าหากัน สร้างสัมพันธ์อันดี ช่วยเหลือเกื้อกูลกัน

เพื่อให้ค่านิยมเชิงบวกต่อชุมชน และสังคมมีความยั่งยืน จึงควรปฏิบัติตาม

แนวทางการใช้เทคโนโลยีให้เหมาะสมด้วยตัวเอง

1) ตระหนักถึงผลผลกระทบของการกระทำของตนเอง

ควรคิดถึงผลจากการกระทำการของตนเอง ก่อนที่จะโพสต์ข้อความ หรือแชร์ ข้อมูลใด ๆ บนโลกออนไลน์

2) ให้ความเคารพผู้อื่น

ไม่ใช้คำพูดหรือการกระทำที่เป็นการเหยียดหยามหรือล่วงละเมิดผู้อื่น

3) ใช้เทคโนโลยีอย่างสร้างสรรค์

ใช้เพื่อสร้างสรรค์สิ่งใหม่ ๆ เป็นประโยชน์ต่อชุมชนและสังคม

4) มีส่วนร่วมในกิจกรรมเพื่อสังคม

สร้างความสัมพันธ์ที่ดีและช่วยเหลือซึ่งกันและกัน เช่น การบริจาคเงินหรือสิ่งของ การให้ความช่วยเหลือผู้ประสบภัย หรือการสนับสนุนโครงการเพื่อสังคม

ตัวอย่างการใช้เทคโนโลยีที่เหมาะสม เพื่อส่งเสริมค่านิยม เชิงบวกต่อชุมชนและสังคม

1) ใช้เทคโนโลยีเพื่อการศึกษา

เรียนรู้สิ่งใหม่ ๆ พัฒนาความรู้ความสามารถของตนเอง และแบ่งปันความรู้กับผู้อื่นได้

2) ใช้เทคโนโลยีเพื่อช่วยให้ทำงาน

อย่างมีประสิทธิภาพมากขึ้น และสามารถทำงานร่วมกับผู้อื่นจากทั่วโลกได้

3) ใช้เทคโนโลยีเพื่อการทำงานอาสา

สามารถใช้เทคโนโลยีเพื่อช่วยเหลือผู้อื่น แก้ปัญหาในชุมชน และสร้างสังคมที่ดีขึ้น

ผลกระทบที่เกิดขึ้นจาก การใช้เทคโนโลยีที่ไม่เหมาะสม

เราต้องระมัดระวังผลกระทบที่เกิดขึ้นจากการใช้เทคโนโลยีที่ไม่เหมาะสม ซึ่งสามารถแบ่งออกได้เป็น 3 ประเภทหลัก ๆ ดังนี้

01



ผลกระทบต่อตัวผู้ใช้ ได้แก่

- ปัญหาสุขภาพกายและสุขภาพจิต เช่น โรคอ้วน โรคนอนไม่หลับ โรคซึมเศร้า โรคติดสมาร์ตโฟน โรคหลอดเลือดสมอง
- ปัญหาทางสังคม เช่น การติดเกม กลั่นแกล้งทางไซเบอร์ การสูญเสียความเป็นส่วนตัว เป็นต้น

02



ผลกระทบต่อผู้อื่น ได้แก่

- ปัญหาอาชญากรรม เช่น การหลอกลวง การโจรมรัม ข้อมูล การเผยแพร่ข้อมูลเท็จ
- ปัญหาสังคม การแพร่กระจายเนื้อหาที่ไม่เหมาะสม เช่น สื่อตามก่อนajar ความรุนแรง เหยียดเชื้อชาติ เป็นต้น

03



ผลกระทบต่อสังคม ได้แก่

- ปัญหาสิ่งแวดล้อม เช่น การใช้พลังงานไฟฟ้ามาก เกินไป ปัญหายาเสื่อมหลักทรัพย์
- ปัญหาเศรษฐกิจ เช่น การสูญเสียงาน ปัญหาความเหลื่อมล้ำทางสังคม เป็นต้น

แนวทางในการสร้างความตระหนักรถึงผลกระทบ



ที่เกิดขึ้นจากการใช้เทคโนโลยีที่ไม่เหมาะสม

ขอแนะนำแนวทางในการสร้างความตระหนักรถึงผลกระทบที่เกิดขึ้นจากการใช้เทคโนโลยีที่ไม่เหมาะสม ได้แก่

1) การให้ความรู้และความเข้าใจ

เกี่ยวกับผลกระทบของการใช้เทคโนโลยีที่ไม่เหมาะสม

2) การปลูกฝังค่านิยมและจริยธรรม

ในการใช้เทคโนโลยี และหลีกเลี่ยงการใช้เทคโนโลยีในทางที่ก่อให้เกิดโทษ

3) การพัฒนาภูมายและภูมิเบี่ยงที่เกี่ยวข้อง

เพื่อคุ้มครองผู้ใช้เทคโนโลยีและสังคมจากผลกระทบที่อาจเกิดขึ้น

อีกอย่างที่สำคัญคือต้องรู้จักเลือกรับเนื้อหาที่เหมาะสม เพื่อให้ได้รับข้อมูล ที่ถูกต้อง และจะได้มีเผยแพร่ข้อมูลที่อาจก่อให้เกิดผลเสียสู่สังคม



ประโยชน์การใช้เทคโนโลยีเพื่อยกระดับคุณภาพชีวิต

การยกระดับชีวิตผู้คนในทุกด้าน คือ ประโยชน์ที่ชัดเจนของเทคโนโลยีดิจิทัลในปัจจุบัน แต่เราได้เปิดให้ประโยชน์เหล่านี้เข้ามาในชีวิตของเราแล้วหรือยัง ?

1) การเพิ่มโอกาสทางการศึกษา



- การเรียนออนไลน์ ช่วยให้ผู้คนสามารถเข้าถึงการศึกษา และการเรียนรู้ได้มากขึ้น และเป็นทางเลือกที่ได้รับความนิยมในปัจจุบัน เนื่องจากสามารถเรียนได้ทุกที่ทุกเวลา เพียงแค่มีอินเทอร์เน็ต นอกจากนี้ ยังมีแอปพลิเคชันมากมาย ที่ให้บริการการศึกษา ซึ่งจะช่วยให้ผู้คนสามารถเรียนรู้ทักษะต่าง ๆ ได้ด้วยตัวเอง เช่น ทักษะภาษาต่างประเทศ ทักษะการเขียนโค้ด ทักษะในการบริหารจัดการ ทักษะทางด้านวิทยาศาสตร์ เทคโนโลยี วิศวกรรมศาสตร์ คณิตศาสตร์ ทักษะศิลปะ เป็นต้น

2) การเพิ่มรายได้



- เทคโนโลยีช่วยให้ผู้คนสามารถประกอบอาชีพ ได้หลากหลายช่องทางมากขึ้น การขายสินค้าออนไลน์ เป็นช่องทางที่ได้รับความนิยมอย่างมากในการเพิ่มรายได้ในปัจจุบัน สามารถขายสินค้าได้โดยไม่ต้องมีหน้าร้าน เพียงแค่มีสมาร์ตโฟน หรือคอมพิวเตอร์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ สามารถเริ่มต้นขายสินค้าได้ทันที เช่น การให้บริการขนส่ง ผู้คนสามารถให้บริการขนส่งสินค้าหรือผู้โดยสารได้ โดยใช้รถยกหรือรถจักรยานยนต์ของตนเอง

การรับจ้างทำงานผ่านแพลตฟอร์มต่าง ๆ ปัจจุบันมีแพลตฟอร์มมากมาย ที่ให้บริการรับจ้างทำงาน ผู้คนสามารถสมัครใช้บริการเหล่านี้เพื่อทำงาน ทำ เช่น งานเขียนบทความ งานออกแบบ งานแปล งานกราฟิก เป็นต้น

3) การยกระดับคุณภาพชีวิต



- การเข้าถึงบริการสาธารณสุขได้สะดวกและรวดเร็วขึ้น การนัดหมายแพทย์ออนไลน์ ช่วยให้ผู้คนสามารถนัดหมายแพทย์ได้โดยไม่ต้องเดินทางไปโรงพยาบาล ประหยัดเวลาในการรอคิวยังช่วยให้วางแผนในการเดินทางได้ง่ายขึ้น
- การตรวจสอบทางไกล ปัจจุบันผู้คนสามารถปรึกษาแพทย์และรับการรักษาได้จากที่บ้าน โดยไม่ต้องเดินทางไปโรงพยาบาล

นอกจากนี้ เทคโนโลยียังช่วยให้ผู้คนสามารถดูแลสุขภาพตนเองได้มากขึ้น เช่น ดูคลิปสอนออกกำลังกาย หรือใช้อแอปพลิเคชันติดตามสุขภาพที่จะค่อยติดตามสุขภาพของเรา เช่น อัตราการเต้นของหัวใจ ระดับน้ำตาลในเลือด ปริมาณแคลอรีที่บริโภค หรืออุปกรณ์ติดตามการออกกำลังกายที่ช่วยนับจำนวนก้าวที่เดิน ระยะทางที่วิ่ง หรือระยะเวลาที่ออกกำลังกายเป็นต้น

เทคโนโลยีเป็นเครื่องมือที่ทรงพลัง ที่สามารถช่วยให้ผู้คนยกระดับชีวิตในด้านต่าง ๆ ได้ สิ่งสำคัญคือ ควรมีความรู้ความเข้าใจในการใช้เทคโนโลยีอย่างมีประสิทธิภาพและปลอดภัย เพื่อให้ได้รับประโยชน์สูงสุด



การสืบค้นข้อมูล จากสื่อดิจิทัล



การสืบค้นข้อมูลจากสื่อดิจิทัลสามารถแบ่งออกเป็นประเภทหลัก ๆ คือ

1 การสืบค้นด้วยคำค้น (Keyword Search)

เป็นวิธีการสืบค้นแบบพื้นฐานที่ได้รับความนิยมมากที่สุด โดยการพิมพ์คำหรือวลีที่ต้องการลงในช่องค้นหาของโปรแกรมค้นหา (Search Engine) แล้วโปรแกรมค้นหาจะประมวลผลคำค้นและแสดงผลการค้นหาที่ตรงกับคำค้นนั้น ๆ ออกมา

2 การสืบค้นขั้นสูง (Advanced Search)

เป็นวิธีการสืบค้นที่ช่วยให้ผู้ใช้สามารถค้นหาข้อมูลที่ต้องการ ได้ละเอียดและเฉพาะเจาะจงยิ่งขึ้น โดยสามารถกำหนดเงื่อนไขในการสืบค้นได้ เช่น ประเภทของไฟล์ ภาษา ช่วงเวลา เป็นต้น

นอกจากนี้ ยังมีวิธีการสืบค้นแบบอื่น ๆ ที่น่าสนใจ เช่น

1) การสืบค้นด้วยเสียง (Voice Search)

ใช้เสียงแทนการพิมพ์คำค้น โดยผู้ใช้สามารถพูดคำหรือวลีที่ต้องการค้นหาลงในไมโครโฟนของโปรแกรมค้นหา

2) การสืบค้นภาพ (Image Search)

เป็นวิธีการสืบค้นโดยใช้ภาพแทนการพิมพ์คำที่ต้องการค้น โดยอัปโหลดภาพที่ต้องการค้นหาลงในโปรแกรมค้นหา

การสืบค้นข้อมูลจากสื่อดิจิทัล อย่างมีประสิทธิภาพ



1. กำหนดวัตถุประสงค์ในการสืบค้น

ว่าต้องการข้อมูลเกี่ยวกับอะไร ต้องการข้อมูลประเภทใด มีความถูกต้องและความน่าเชื่อถือมากน้อยเพียงใด

2. กำหนดคำหรือวลีที่ต้องการค้นหา

ใช้คำที่มีความหมายเฉพาะเจาะจง
และครอบคลุม



3. ใช้เทคนิคการสืบค้นขั้นสูง

หากต้องการค้นหาข้อมูลที่ต้องการ
ได้อย่างละเอียดและเฉพาะเจาะจงยิ่งขึ้น

4. ประเมินผลการค้นหา

โดยพิจารณาจากแหล่งที่มาของข้อมูล ความถูกต้องของ
ข้อมูล และแหล่งอ้างอิง การสืบค้นข้อมูลจากสื่อดิจิทัล
เป็นทักษะที่จำเป็นสำหรับทุกคน อย่างไรก็ตาม เรายัง
ใช้ทักษะนี้อย่างชำนาญฉลาด ตรวจสอบความถูกต้องของ
ข้อมูลและแหล่งที่มาของข้อมูลอย่างรอบคอบ เพื่อไม่ให้
ถูกหลอกลวงหรือตกเป็นเหยื่อของข้อมูลเท็จ



เครื่องมือในการค้นข้อมูลจากสื่อดิจิทัล

เครื่องมือที่ใช้ในการค้นหาข้อมูลทั่วไป

- **Google Search (Google):**

เป็นเครื่องมือค้นหาที่แพร่หลายที่สุด มีความสามารถในการค้นหาโดยใช้ อัลกอริทึมที่ทันสมัย

- **Microsoft Bing :**

เป็นเครื่องมือค้นหาอีกตัวที่มีความสามารถในการค้นหาข้อมูลทั่วไป และ รูปภาพ

- **Yahoo Search:**

เครื่องมือค้นหาที่มีให้บริการค้นหาข้อมูลและเนื้อหาทางอินเทอร์เน็ต

- **DuckDuckGo:**

เน้นการค้นหาโดยที่ไม่ติดตามการใช้งานของผู้ใช้ เพื่อเพิ่มความเป็นส่วนตัว

เครื่องมือที่ใช้ ในการค้นหาข้อมูลเกี่ยวกับสื่อบันเทิงและสังคม

- **YouTube:**

สำหรับค้นหาวิดีโอ

- **Social Media Platforms:**

ในการค้นหาข้อมูลที่เกี่ยวข้องกับสังคมและเหตุการณ์ที่เกิดขึ้น

เครื่องมือที่ใช้ในการค้นหาข้อมูลทางการศึกษา

Wolfram Alpha ให้บริการค้นหาข้อมูลทางการคณิตศาสตร์และวิทยาศาสตร์

เครื่องมือค้นหาทางวิทยาศาสตร์

สำหรับการค้นหาข้อมูลทางวิทยาศาสตร์และการแพทย์ เช่น Google Scholar, PubMed

เครื่องมือค้นหาและวิเคราะห์ข้อมูล

ใช้สำหรับค้นหาและนำเสนอข้อมูลในรูปแบบที่เข้าใจง่าย

เครื่องมือค้นหาหนังสือ

สำหรับการค้นหาข้อมูลในหนังสือและสืบพิมพ์ เช่น Google Books, Amazon

เครื่องมือค้นหารูปภาพ

ให้บริการค้นหารูปภาพและข้อมูลที่เกี่ยวข้อง เช่น Google Images, TinEye

เครื่องมือค้นหาสื่อเสียง

สำหรับค้นหาเพลงและสื่อเสียง เช่น Spotify, Apple Music

ทั้งนี้การเลือกเครื่องมือในการค้นข้อมูลจากสื่อดิจิทัลที่เหมาะสมขึ้นอยู่กับวัตถุประสงค์ในการสืบค้น เราควรพิจารณาปัจจัยต่าง ๆ ก่อนสืบค้นเพื่อความสะดวกรวดเร็วและมีประสิทธิภาพ



เคล็ดลับที่ไม่ลับ

เทคนิคการค้นหาข้อมูลจากสื่อดิจิทัลอย่างไรให้ตรงใจ

ทำให้ได้ข้อมูลที่ต้องการและช่วยให้ชีวิตเราง่ายขึ้น มาดูวิธีการกันเลย

1) กำหนดคำค้น

หรือคีย์เวิร์ด ให้กระซับ ชัดเจน และครบถ้วนมากที่สุด

2) เลือกเครื่องมือค้นหา

ที่เหมาะสมมากที่สุด

3) ใช้เทคนิคในการช่วยสืบค้นขั้นสูง (Advanced Search)

ดังต่อไปนี้

ค้นโดยกำหนดไฟล์ที่ต้องการ:

ด้วยการใส่คำว่า **filetype:** ตามด้วยนามสกุลของไฟล์ ตัวอย่าง สมัครงาน
 filetype:doc

ค้นแบบเจาะจงเว็บไซต์:

ค้นหาด้วย **site:** ชื่อเว็บไซต์ คำค้นตัวอย่าง **site: www.dsdb.go.th**

ค้นโดยให้มีคำค้นทุกคำในแหล่งเดียว

ให้ใส่คำค้นทุกคำที่ต้องการโดยเว้นวรคระหว่างคำค้น ตัวอย่าง สมัครงานกราฟิก ซองนทรี

ค้นโดยใช้คำช่วย OR

กรณีอยากรู้ได้ข้อมูลเพิ่มมากขึ้นเกี่ยวกับคำค้นหลัก ตัวอย่าง สมัครงานกราฟิก OR 2D Animator

ใส่เครื่องหมายคำพูด

กรณีต้องการให้มีห้องประโภคในแหล่งข้อมูล ตัวอย่าง "Work From Home"

ใส่เครื่องหมายลบ

เพื่อกรองคำที่ไม่ต้องการออก โดยใส่ คำค้น - คำที่ต้องการกรองออก ตัวอย่าง กราฟิก - ตัดต่อ

แปลงหน่วยต่าง ๆ

โดยพิมพ์ ตัวเลข หน่วยก่อนแปลง เท่ากับ หน่วยหลังแปลง อย่างเช่น แปลงค่าเงิน ตัวอย่างคำค้น 100 บาท เท่ากับ ดอลลาร์

แสดงเวลาเปรียบเทียบ

เวลา ประเทศไทย 1 ประเทศไทย 2 ตัวอย่าง เวลา ไทย อเมริกา

เพียงเท่านี้เราก็จะสามารถสืบค้นข้อมูลได้อย่างตรงใจมากขึ้น !



TIP

เคล็ดลับการค้นหาข้อมูลออนไลน์ คุณเคยลองแล้วหรือยัง?

(เรียนรู้จากข้อมูลคำแนะนำของ Google Gemini)



เทคนิคขั้นพื้นฐาน

1. ใช้คำค้นหาที่เฉพาะเจาะจง

แทนที่จะพิมพ์ "แมว" ลองพิมพ์ "แมวไทย" หรือ "สายพันธุ์แมว"

2. ใช้เครื่องหมายคำพูด ("")

เช่น "คำว่ารักไม่เคยแพ้อะไร" เพื่อค้นหาเฉพาะวารีสัน

3. ใช้เครื่องหมายลบ (-)

เช่น "รถยนต์ - มือสอง" เพื่อไม่ให้แสดงผลลัพธ์เกี่ยวกับรถยนต์มือสอง

4. ใช้เครื่องหมายบวก (+)

เช่น "ข่าว + ดิจิทัลไอเดีย" เพื่อบังคับให้มีคำว่า "ดิจิทัลไอเดีย" ในผลลัพธ์

5. ค้นหาภายในเว็บไซต์ (site:)

เช่น "site:wikipedia.org ประเทศไทย" เพื่อค้นหาคำว่า ประเทศไทย
เฉพาะใน Wikipedia



TIP

6. ใช้ตัวกรองการค้นหา

เช่น กรองตามวันที่ เพื่อดูผลลัพธ์ในช่วงวันที่ต้องการ

7. ลองเครื่องมือค้นหาอื่น

เช่น DuckDuckGo เน้นความเป็นส่วนตัวมากกว่า Google หรือ Bing Yandex หรือ Baidu ที่อาจมีผลการค้นหาที่เสริมกัน

8. ตรวจสอบแหล่งที่มา

เช่น ดูว่าเว็บไซต์เป็นขององค์กรที่น่าเชื่อถือหรือไม่
 ไม่หลงเข้าในครั้งแรกที่เห็น

9. ใช้คำพ้องความหมาย

เช่น "วิธีทำ" หรือ "สูตร" แทนคำว่า "ทำอย่างไร"

10. ใช้เครื่องหมายดอกจัน (*)

เช่น "วิธีทำ*ผัดไทย" เพื่อค้นหาสูตรอาหารผัดไทยทุกประเภท

**TIP**

เทคนิคขั้นสูง



1. ใช้ประโยชน์จากฟังก์ชัน autocomplete

พิมพ์แค่คำหรืออักษรต้น แล้วลองใส่ดูคำที่เครื่องมือค้นหาแนะนำให้มา

2. เรียนรู้คีย์ลัด

เช่น Ctrl+F เพื่อค้นหาคำในหน้าเว็บ หรือ Ctrl+T เพื่อเปิดแท็บใหม่

3. ใช้เครื่องมือบุกมาร์ก

เก็บเว็บไซต์ที่เป็นประโยชน์ไว้ดูภายหลัง

4. อัปเดตความรู้การค้นหาอยู่เสมอ

ติดตามข่าวสารและเทคนิคใหม่ ๆ รวมทั้งการใช้ AI ในการสืบค้นเรียนรู้เรื่องข้อมูล

5. ใช้เครื่องมือค้นหาเฉพาะด้าน

เช่น PubMed สำหรับงานวิจัยทางการแพทย์

6. ใช้เครื่องมือค้นหาเชิงวิชาการ

เช่น Google Scholar สำหรับบทความวิชาการ

7. ใช้ Boolean operators (AND, OR, NOT)

เช่น "แมว AND สุนัข" เพื่อค้นหาข้อมูลที่มีทั้งแมวและสุนัข

8. ใช้เครื่องมือค้นหาเฉพาะ

เช่น Wolfram Alpha สำหรับคำนวณ หรือ Wayback Machine เพื่อดูเว็บไซต์ในอดีต



TIP

9. ค้นหาจากแหล่งข้อมูลที่หลากหลาย

ไม่จำกัดด้วยแค่เว็บไซต์ ลองค้นหาในหนังสือ วารสาร หรือฐานข้อมูลอื่น ๆ

10. ค้นหาด้วยเสียง

ใช้การค้นหาด้วยเสียงเมื่อสะดวก

11. ใช้การค้นหาด้วยรูปภาพ

อัปโหลดรูปภาพเพื่อค้นหาข้อมูลที่เกี่ยวข้อง

12. ใช้เครื่องมือค้นหาสำหรับการซืบปิง

เช่น Google Shopping เพื่อเปรียบเทียบราคาสินค้า

13. ใช้เครื่องมือค้นหาสำหรับการท่องเที่ยว

เช่น Kayak หรือ Skyscanner เพื่อค้นหาตัวเครื่องบินและโรงแรม

14. ใช้เครื่องมือค้นหาสำหรับการเรียน

เช่น Google Scholar หรือ JSTOR สำหรับบทความวิชาการ

15. ใช้เครื่องมือค้นหาสำหรับการทำงาน

เช่น LinkedIn หรือ Indeed

16. ใช้เครื่องมือค้นหาสำหรับการเรียนภาษา

เช่น Duolingo หรือ Memrise

17. ใช้เครื่องมือค้นหาสำหรับการค้นหาสูตรอาหาร

เช่น Yummly หรือ Allrecipes



TIP

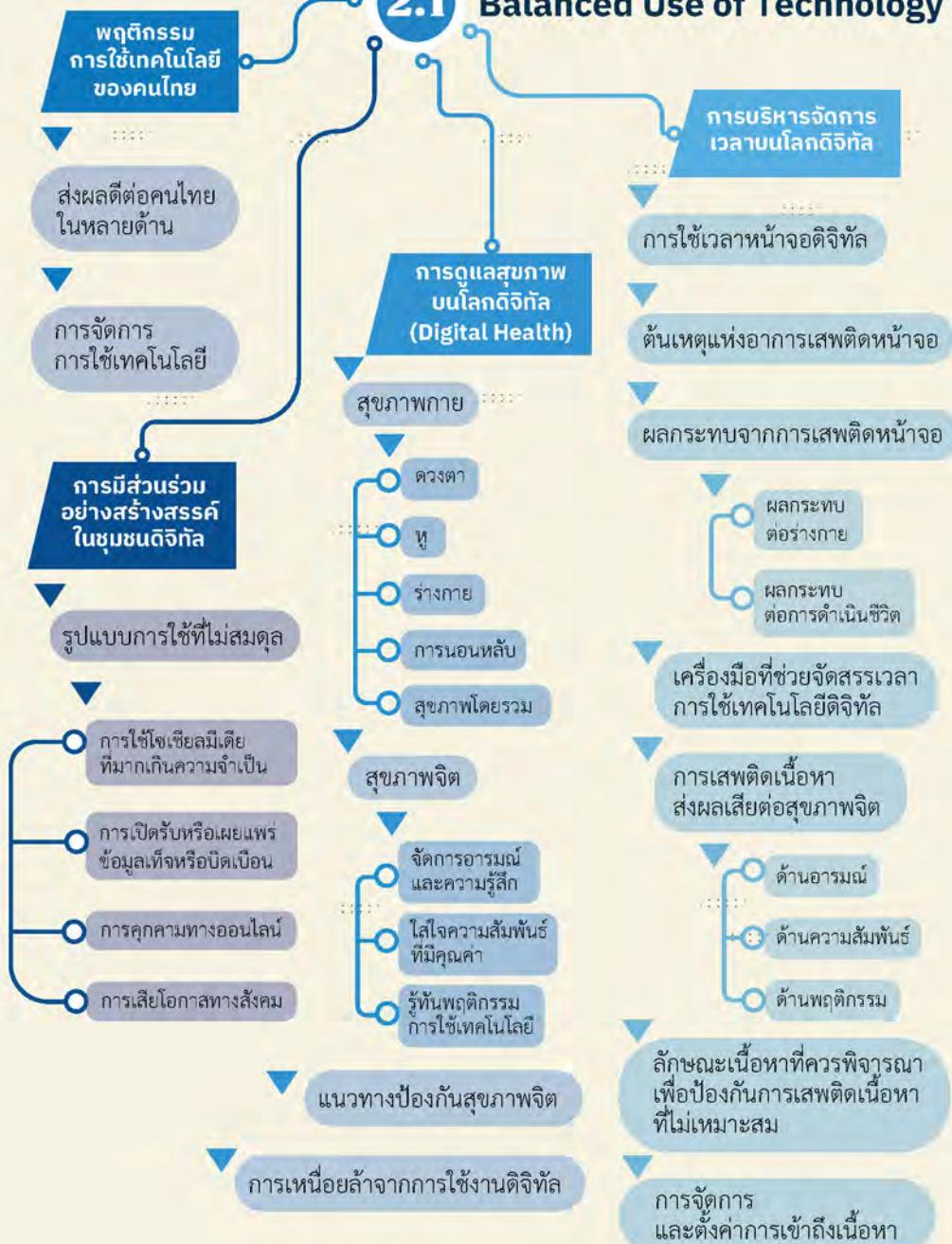
18. ใช้เครื่องมือค้นหาสำหรับการค้นหาภาพยนตร์และรายการทีวี เช่น IMDb หรือ Rotten Tomatoes
19. ใช้เครื่องมือค้นหาสำหรับการค้นหาเพลง เช่น Spotify หรือ Apple Music
20. ใช้เครื่องมือค้นหาสำหรับการค้นหาหนังสือ เช่น Goodreads หรือ LibraryThing
21. ใช้เครื่องมือค้นหาสำหรับการค้นหาข้อมูลการเดินทาง เช่น TripAdvisor หรือ Lonely Planet
22. ใช้เครื่องมือค้นหาสำหรับการค้นหาข่าวสาร เช่น Google News หรือ Apple News
23. ใช้เครื่องมือค้นหาสำหรับการค้นหาข้อมูลเกี่ยวกับสุขภาพ เช่น WebMD หรือ Mayo Clinic
24. ใช้เครื่องมือค้นหาสำหรับการค้นหาข้อมูลเกี่ยวกับการเงิน เช่น Yahoo Finance หรือ Google Finance
25. ใช้เครื่องมือค้นหาสำหรับการค้นหาข้อมูลเกี่ยวกับกีฬา เช่น ESPN หรือ Bleacher Report
26. ใช้เครื่องมือค้นหาสำหรับการค้นหาข้อมูลเกี่ยวกับเทคโนโลยี เช่น TechCrunch หรือ The Verge



เทคโนโลยีช่วยให้เราได้ติดต่อ
รังสรรค์ก่อสังคมเชื่อมพسانผสม
ทั้งตอบโต้ติดตามความนิยม
รายการความเห็นคอมเมนต์กัน
สิ่งสำคัญพึงระวังถึงใจเขา
อย่าหยอกเย้ายุ้งແย่งແย়েং যে যাহন
ค่านิยมสามัคคีผูกสัมพันธ์
ร่วมแบ่งปันสีบคันข้อเท็จจริง

2.1

Balanced Use of Technology



2.2 Civic Use of Technology

การใช้เทคโนโลยี
ในสื่อดิจิทัล
เพื่อสังคม และตัวเอง

รูปแบบการใช้เทคโนโลยี

การจัดการผลกระทบ
จากการใช้งานเทคโนโลยีดิจิทัล

ผลกระทบ
ทางบวก

ผลกระทบ
ทางลบ

แนวทางการใช้เทคโนโลยี
อย่างเหมาะสม

การเอาใจเข้า
มาใส่ใจเราทางดิจิทัล

แนวทางการพัฒนาทักษะ
Digital Empathy

การรับมือกับสถานการณ์
ที่กระทบต่อความรู้สึก

ไม่ควรทำ

ควรทำ

การใช้เทคโนโลยี
อย่างเหมาะสม

ค่านิยมเชิงบวกในการใช้
เทคโนโลยีให้เหมาะสม

แนวทางการใช้เทคโนโลยี
ให้เหมาะสมด้วยตัวเอง

ตัวอย่างการใช้เทคโนโลยี
ที่เหมาะสม

ผลกระทบที่เกิดขึ้น
จากการใช้เทคโนโลยี
ที่ไม่เหมาะสม

แนวทางในการสร้าง
ความตระหนักถึงผลกระทบ

ประโยชน์การใช้เทคโนโลยี
เพื่อกระตับคุณภาพชีวิต

การสืบค้นข้อมูล
จากสื่อดิจิทัล

การสืบค้นข้อมูล
จากสื่อดิจิทัล
อย่างมีประสิทธิภาพ

เครื่องมือในการค้นข้อมูล
จากสื่อดิจิทัล

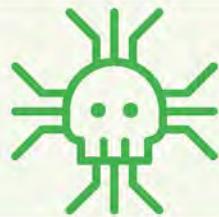
เทคนิคการค้นหาข้อมูล
จากสื่อดิจิทัลอย่างไร
ให้ตรงใจ

เคล็ดลับการค้นหา
ข้อมูลออนไลน์

เทคนิคขั้นพื้นฐาน

เทคนิคขั้นสูง

03



การจัดการความปลอดภัย ในโลกดิจิทัล

— Digital Security —

ແນະນຳສໍາຮັບຜູ້ສວນ



- **ວັດຖປະສົງຄົມ**

ຜູ້ເຮືອນມີຄວາມຮູ້ເກີ່ວກັບ ຄວາມເສື່ອງ ການປຶກປັງກັນ ອີເກມ ຂໍ້ອກຈັດການ
ກັບຄຸກຄາມທາງໃຊ້ເບຼອຣີດີ

- **ຂອບເຂຕຂອງເນື່ອຫາດ້ານນີ້**

3.1 Behavioral Cyber-Risk Management



ຄວາມປລອດກັຍເຮີມທີ່ການປກປຶກ “ສ່ວນບຸກຄົດ”

ວັນທີສອນ
/ / /



ການລ່ວງລະເມີດທາງໃຊ້ເບຼອຣີ (Cyber Abuse)

ວັນທີສອນ
/ / /



ກັບຄຸກຄາມທາງໃຊ້ເບຼອຣີ (Cyber Threat)

ວັນທີສອນ
/ / /



ອອນໄລນ໌ຍ່າງໄວໃໝ່ປລອດກັຍ ?

ວັນທີສອນ
/ / /

● ขอบเขตของเนื้อหาด้านนี้

3.2 Organizational Cyber-Risk Management



First Jobber ครรภ์ไว้ !

วันที่สอน
/ / /



ความเสี่ยงจากการใช้เทคโนโลยีในองค์กร

วันที่สอน
/ / /



แนวปฏิบัติเพื่อร่วมกันป้องกันภัยไซเบอร์ระดับองค์กร

วันที่สอน
/ / /



กฎหมายที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ในประเทศไทย

วันที่สอน
/ / /

เวลาในการเรียน



รู้คัพก ไม่สับสน



2

1



SOCIAL ENGINEERING

หรือ วิถีการหลอกลวงคน

คือ เป็นศิลปะการหลอกลวงผู้คน เพื่อผลประโยชน์ตามที่ขอยกเว้นต้องการ โดยใช้วิธีทางจิตวิทยาในการหลอกล่อ



TECHNICAL ATTACKS

คือ ภัยคุกคามจากผู้มีความรู้ด้านระบบคอมพิวเตอร์เครือข่าย และข้อมูลทางอิเล็กทรอนิกส์

4



RANSOMWARE

คือ ภัยคุกคามทางไซเบอร์ที่ทำการเข้ารหัส หรืออีคลิฟฟ์ ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ โดยผู้ใช้งานจะไม่สามารถ เปิดไฟล์ได้ ฯ ได้เลย หากไฟล์เหล่านั้นถูกเข้ารหัส และเพื่อกู้ข้อมูลคืน ผู้ใช้งาน จะต้องทำการจ่ายเงินตามที่ความ “เรียกค่าไถ่” ที่ปรากฏ



SYNTHETIC CONTENT

หรือ ข้อมูลสังเคราะห์

คือข้อมูลที่ไม่ได้สร้างขึ้นโดยมนุษย์ ซึ่งเลียนแบบข้อมูลในโลกแห่งความเป็นจริง ข้อมูลประเภทนี้จะสร้างขึ้นจากอัลกอริทึม การประมวลผล และการจำลองโดยใช้เทคโนโลยีปัญญาประดิษฐ์ช่วยสร้าง

รู้คัพก ไม่สับสน



5

**SCAMS**

คือ ลักษณะการหลอกลวงในรูปแบบต่าง ๆ
ผ่านระบบอินเทอร์เน็ต

6

**WATERMARK**

หรือลายน้ำ

คือ การแสดงความเป็นเจ้าของรูปภาพ
หรือเอกสารนั้น ๆ โดยลายน้ำมีลักษณะ
ที่เป็นรูปภาพจาง ๆ ที่สามารถอ่านงบน
ส่วนใหญ่ของรูปภาพหรือข้อความก็ได้

7

**PASSKEY**

คือ เป็นวิธีล็อกชื่อเข้าบัญชีผู้ใช้ในเว็บไซต์
หรือในแอปพลิเคชันโดยพิสูจน์ตัวผู้ใช้
(AUTHENTICATION) โดยไม่ต้องมีรหัสผ่าน



ถ้าคุณเรียนผ่านด้านนี้
คุณจะรู้จัก
เข้าใจและป้องกันตนเอง
จากภัยคุกคามทางไซเบอร์ ได้

3.1

BEHAVIORAL CYBER-RISK MANAGEMENT

วัตถุประสงค์

- ผู้เรียนสามารถตระหนักรถึงความเสี่ยงหรือความไม่ปลอดภัยที่อาจเกิดขึ้นบนโลกดิจิทัล
- ผู้เรียนรู้วิธีการออนไลน์ให้ปลอดภัยและตั้งรหัสผ่านอย่างไรให้ปลอดภัย
- ผู้เรียนสามารถเข้าใจถึงการป้องกันหรือการจัดการภัยคุกคามทางไซเบอร์ได้

ทำอย่างไร ? เราจึงจะปลอดภัยในโลกดิจิทัล

ไม่มีสิ่งใดสิ่งเดียวจะเป็นคำตอบได้ เหมือนกับการขับขี่ยานพาหนะบนท้องถนน ที่ความปลอดภัยไม่ได้ถูกกำหนดโดยฝ่ายใดฝ่ายเดียว

ดังนั้น การรับประกันความปลอดภัยในโลกดิจิทัลจึงเป็นความร่วมมือกันของแต่ละบุคคล ตลอดจนองค์กร และระบบในภาพรวม

ในหลักสูตร EDC Plus ด้านที่ 3 นี้ เราจะร่วมกันมองไปที่ 2 ส่วนสำคัญอันเป็นฐานของการสร้างความปลอดภัยในโลกดิจิทัลให้เกิดขึ้นทั้งต่อตนเอง และสังคม

เริ่มต้นจากเรื่องราวของ “พฤติกรรม” ส่วนตัวแต่ละบุคคล ทั้งหมดรวมอยู่ในบทที่ 3.1 Behavioral Cyber-Risk Management จัดการความเสี่ยงไซเบอร์ส่วนบุคคล

ถัดจากนั้น เราจะขยายวงสู่การป้องกันตนให้พ้นจากการถูกโจมตีทางไซเบอร์ ในฐานะที่เราแต่ละคน ล้วนอยู่ในบทบาทปราการปกป้ององค์กรพร้อมเทคนิคความปลอดภัยออนไลน์ง่าย ๆ แต่ช่วยลดความเสี่ยงได้อย่างมาก ติดตามใน 3.2 Organizational Cyber-Risk Management จัดการความเสี่ยงไซเบอร์ระดับองค์กร



ความปลอดภัยเริ่มที่



การปกป้อง ✓

“ส่วนบุคคล”

ความเสี่ยงภัยทางไซเบอร์ส่วนบุคคล เกิดขึ้นในหลากหลายรูปแบบ จัดกลุ่มได้เป็นสองส่วน คือ การล่วงละเมิดทางไซเบอร์ (Cyber Abuse) และ การคุกคามทางไซเบอร์ (Cyber Threat)

การล่วงละเมิดทางไซเบอร์

เป็นการกระทำที่สร้างผลร้ายต่อบุคคลในด้านจิตใจ ตัวตน ตลอดจนเชื่อมโยงสู่ผลลัพธ์ทางร่างกายและชีวิตรักษาสุขภาพ

ข่าวร้ายคือ หากเราไม่ตระหนักรายครั้งเรารอาจถูกหลอกเข้าไปผู้ล่วงละเมิดผู้อื่นโดยไม่ตั้งใจ

การคุกคามทางไซเบอร์

เป็นการกระทำที่ก่อความเสียหายต่อทรัพย์สิน ระบบ อุปกรณ์ ซึ่งอาจเรียกว่าเป็นการโจรกรรม

ที่น่าเสียดายคือ หลายครั้งความเสียหายเกิดขึ้น เพราะช่องโหว่ที่เราเปิดไว้เอง เมื่อฉันกับรายนั้นที่เปิดประตูค้างไว้แมมยังเสียบกุญแจมาไว้ให้ด้วย

การล่วงละเมิด ทางไซเบอร์ (Cyber Abuse)



การล่วงละเมิดทางไซเบอร์ (Cyber Abuse)

คือ การใช้เทคโนโลยีดิจิทัลเพื่อคุกคาม ข่มขู่ หรือก่อการผู้อื่นในทางที่เป็นอันตราย หรือไม่เหมาะสม

รูปแบบการล่วงละเมิดทางไซเบอร์

สามารถเกิดขึ้นในหลายรูปแบบ เช่น

1. การคุกคามทางอิเล็กทรอนิกส์ (Cyberstalking)

การติดตามหรือก่อการผู้อื่นอย่างต่อเนื่องผ่านช่องทางออนไลน์ จนทำให้ผู้ถูกติดตาม หรือถูกก่อการ รู้สึกถูกคุกคามหรือไม่ปลอดภัย เช่น



EXAMPLE

ໄວດວລສາວເຈວແພນຄລັບໜາຍຄນເດີມທຸກທີ່ໄປ
ເຂາຕິດຕາມຂ້ອນນູ້ລສາແກ່ເຖິງວິທີໄວດວລໂພສຕີ
ແລ້ວຕິດຕາມໄປທຸກທີ່ ແກນຍັງກຳເໜີວຸນບັງເວີລູເຈວ
ກຳໃຫ້ໄວດວລສາວຮູ້ສັກໄມ່ປລອດກັຍຈນຕ້ອງແຈ້ງຄວາມ

2. การเปิดเผยข้อมูลส่วนตัว (Doxxing)



การเปิดเผยหรือแพร่กระจายข้อมูลส่วนตัว รูปภาพ คลิปวิดีโอ หรือข้อมูลที่ละเอียดอ่อนของบุคคลอื่น โดยไม่ได้รับอนุญาต เช่น

EXAMPLE

การล่าแม่งดหรือคนที่ไม่ชอบบนโลกออนไลน์โดยทำการบุดรูปเก่า ๆ ข้อมูลที่อยู่ที่ทำงานบุคคลรอบตัวออกมาเปิดเผย

3. การกลั่นแกล้งทางไซเบอร์ (Cyberbullying)



การใช้แพลตฟอร์มออนไลน์เพื่อข่มขู่ ล้อเลียน หรือทำร้ายผู้อื่น ทั้งในด้านจิตใจและอารมณ์

4. การใช้คำพูดเกลียดชัง (Hate Speech)



คือการเผยแพร่หรือแสดงความคิดเห็นที่มีเนื้อหาเกลียดชัง ล่วงละเมิด หรือเลือกปฏิบัติต่อบุคคล ซึ่งไม่ได้จำกัดแค่คำพูด แต่รวมไปถึงสื่อทุกชนิด และไม่ได้จำกัดเพียงแค่การใช้ถ้อยคำหยาบคาย ด่าหอ ดูถูกเหยียดหยามเท่านั้น แต่รวมถึงความตั้งใจทำให้ผู้อื่นเข้าใจผิด โน้มน้าวซักจุ่งให้เกลียดชังเป็นอย่างมาก ตลอดจนการลดTHONศักดิ์ศรีและคุณค่าความเป็นมนุษย์

สาเหตุของการล่วงละเมิดทางไซเบอร์

มีหลายปัจจัยที่ซับซ้อน และเกี่ยวข้องกัน ดังนี้

1. ความไม่ระบุตัวตน :

อินเทอร์เน็ตและโซเชียลมีเดียมักให้ความไม่ระบุตัวตนแก่ผู้ใช้ ซึ่งอาจทำให้บางคนรู้สึกว่า พวกรเขารสามารถทำการล่วงละเมิดคนอื่นได้ โดยไม่ต้องรับผิดชอบต่อการกระทำของตนเอง

2. ขาดการควบคุม :

บางครั้งแพลตฟอร์มออนไลน์ อาจขาดกลไกการควบคุมที่เหมาะสม เพื่อป้องกันการล่วงละเมิดทางไซเบอร์

3. ขาดความเข้าใจและการศึกษา :

ผู้ใช้งานอาจไม่เข้าใจถึงผลกระทบ หรือความรุนแรงของการกระทำของตนต่อผู้อื่น หรือไม่รู้จักวิธีการใช้เทคโนโลยีอย่างมีความรับผิดชอบ

4. ความแตกต่างทางลัทธิและวัฒนธรรม :

ความขัดแย้งหรือความไม่เข้าใจระหว่างกลุ่มคน หรือวัฒนธรรมต่าง ๆ

5. รู้สึกไม่เพิงพอใจหรือถูกทอดทิ้ง :



คนที่มีความรู้สึกไม่เพิงพอใจหรือถูกทอดทิ้ง อาจใช้การละเมิดทางไซเบอร์ เป็นวิธีแสดงความไม่พอใจ หรือแสวงหาความสนใจ

6. ความหวาดกลัวและความไม่แน่นอน :



ในสถานการณ์ที่มีความหวาดกลัว เช่น ระหว่างวิกฤตหรือการเปลี่ยนแปลง ทางสังคม บางคนอาจหันไปใช้การล่วงละเมิดทางไซเบอร์ เพื่อแสดงออก หรือเพื่อจัดการกับความรู้สึกของตน





รับมือการคุกคามทางไซเบอร์

แม้ปัจจัยทางเพศจะเป็นเรื่องยากที่จะจัดการ แต่สำหรับครูที่ได้เรียนรู้ผ่านมาถึงจุดนี้ คงมีแนวทางสร้างเกราะป้องกันสำหรับตนเองไว้บ้างแล้ว

ทั้งด้วยการตระหนักว่า มีโอกาสที่เราอาจจะพบเจอกับการล่วงละเมิด หากมีครอพยาภัยเริ่มต้นการล่วงละเมิด เราควรรู้ทันและหลีกเลี่ยง

ขณะเดียวกัน ควรตั้งค่าความเป็นส่วนตัวบนอุปกรณ์ที่ใช้ให้อยู่ในระดับที่เราต้องการ และรอมัดระวังการเปิดซ่อน เผยแพร่ หรือแชร์ข้อมูลส่วนตัวซึ่งอาจจะถูกนำไปใช้เพื่อตั้งต้นให้กับคนก่อการล่วงละเมิด



WARNING

หากเราไม่ระวัง เราอาจถูกถ่ายเป็นผู้ที่ล่วงละเมิดผู้อื่นได้โดยไม่รู้ตัว วิธีพื้นฐานที่จะป้องกันไม่ให้หลงพลาดพลั้ง เราควรหมั่นก่อร่างสร้าง “ความเข้าอกเข้าใจในโลกดิจิทัล” หรือ Digital Empathy ไว้ให้มั่นคง [โดยสามารถติดตามเรื่องนี้ได้ในด้านที่ 2.2 เข้าอกเข้าใจกันผ่าน Digital Empathy]

ภัยคุกคามทางไซเบอร์ (Cyber Threat)



ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง การกระทำใด ๆ ที่มีความตั้งใจที่จะทำลาย บุกรุก หรือทำให้ระบบคอมพิวเตอร์ ข้อมูลดิจิทัล หรือเครือข่ายการสื่อสารต่าง ๆ ได้รับความเสียหาย ซึ่งอาจมาจากบุคคลกลุ่ม หรือแม้กระทั่งประเทศที่มีเจตนาทำร้าย

รูปแบบภัยคุกคามทางไซเบอร์ ในระดับส่วนตัว

แบ่งได้เป็น 2 กลุ่ม คือ กลุ่มที่ใช้ กลยุทธ์ “วิศวกรรมทางสังคม” หรือ Social Engineering หรือเรียกว่า “ล่อ-ลวง-หลอก” กับอีกกลุ่มหนึ่งใช้วิธีทางเทคนิค หรือบางกรณีเป็นการใช้ห้องส่องวิธีร่วมกัน เช่น “หลอกให้เชื่อ เพื่อให้เหยื่อติดตั้งแอป”

สำหรับรูปแบบภัยคุกคามทางไซเบอร์ ในระดับส่วนตัว มีเทคนิคน่าสนใจที่ควรรู้ทัน อาทิ

กลยุทธ์ทางวิศวกรรมสังคม (Social Engineering)

- วงศ์ให้กรอกข้อมูล (Phishing Scams)

การส่งอีเมล หรือสร้างเว็บไซต์ปลอมแปลง เลียนแบบองค์กรที่น่าเชื่อถือ เพื่อหลอกให้ เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น หลอกให้ กรอกรหัสผ่าน เลขบัตรเครดิต



- หลอกให้ดึง (Lottery or Prize Scam)

หลอกให้เหยื่อเชื่อว่า ชนะรางวัล แต่สุดท้ายต้องจ่ายเงิน โ荷ลดแอปฯ หรือมอบข้อมูลส่วนบุคคล



- หลอกให้รัก (Romance Scam)

หลอกให้รัก แล้วออกอุบายเพื่อให้ เหยื่อหลงเชื่อโอนเงินให้



- หลอกให้ลงทุน (Investment Scam)

หลอกให้ลงทุน โดยกล่าวอ้างอย่างน่าเชื่อ ว่าจะได้รับผลตอบแทนสูง

● สวมรอยหลอก (Pretexting)

การสร้างสถานการณ์ปลอมขึ้นมา เพื่อให้เหยื่อไว้ใจ และยอมเปิดเผยข้อมูลส่วนตัว เช่น ปลอมเป็นฝ่ายเทคนิคการสนับสนุน ปลอมเป็นเจ้าหน้าที่ตำรวจ



● วางเหยื่อล่อ (Baiting)



การดึงดูดเหยื่อด้วยข้อเสนอล่อใจเพื่อให้หลงกล เช่น บัตรของขวัญฟรี คูปองส่วนลด สุดพิเศษ เมื่อเหยื่อหลงเชื่อคลิกลิงก์ หรือดาวน์โหลดไฟล์ อาจติดตั้งมัลแวร์ (Malware) หรือถูกนำไปยังเว็บไซต์ที่ขโมยข้อมูลส่วนตัว

● ขู่กรรโชก (Scareware)

การสร้างความเร่งด่วน ปลอมแปลงสถานการณ์ให้เหยื่อรู้สึกกลัว เช่น แจ้งเตือนว่าบัญชีของคุณถูกบุกรุก ข้อมูลของคุณรั่วไหล เพื่อกดดันให้เหยื่อตัดสินใจผิดพลาด เช่น คลิกลิงก์ที่ไม่ปลอดภัยหรือดาวน์โหลดโปรแกรมรักษาความปลอดภัยปลอม



● Mining Social Media

การเรียนรู้และเก็บรวบรวมข้อมูลจากกิจกรรมบนโลกออนไลน์ของเหยื่อ เพื่อนำมาสร้างชุดข้อมูลสำหรับใช้ทำให้เหยื่อหลงเชื่อได้ง่ายขึ้น

กลยุทธ์การโจมตีทางเทคนิค (Technical Attacks)

- **มัลแวร์ (Malware)**

สร้างแอปหรือซอฟต์แวร์ที่ไม่พึงประสงค์ สามารถติดตั้งบนอุปกรณ์โดยไม่รู้ตัว ทำหน้าที่ขโมยข้อมูล ทำลายอุปกรณ์ หรือควบคุมอุปกรณ์ของเราได้



- **การโจมตีแบบ Watering Hole**

ผังมัลแวร์ในเว็บไซต์ที่กลุ่มเป้าหมายมักเข้าใช้งานบ่อย ๆ เพื่อให้อุปกรณ์ของเหยื่อติดตั้งมัลแวร์ทันทีที่เข้าใช้งาน

- **การโจมตีแบบ Zero-Day**

การใช้ช่องโหว่ของซอฟต์แวร์โจมตี ก่อนที่จะมีแก้ไขอย่างช่องโหว่ การโจมตีลักษณะนี้ป้องกันได้ยาก



สาเหตุของภัยคุกคามทางไซเบอร์

เกิดจากหลายสาเหตุที่ซับซ้อนและเชื่อมโยงกัน ปัจจัยต่าง ๆ เหล่านี้ ส่งผลให้เกิดความเสี่ยงและช่องโหว่ ที่ผู้โจมตีสามารถใช้ประโยชน์ เพื่อทำการโจมตีทางไซเบอร์ได้ ต่อไปนี้คือบางสาเหตุหลักของภัยคุกคามทางไซเบอร์

1. อินเทอร์เน็ตสามารถซ่อนตัวตนได้

โดยการทำโปรไฟล์ปลอมขึ้นมา ทำให้บางคนรู้สึกว่าสามารถกระทำการไม่เหมาะสม โดยไม่ต้องเผชิญกับผลที่ตามมาได้



2. หลักการโจมตีทางไซเบอร์มีจุดประสงค์เพื่อการฉ้อโกงทางการเงิน เช่น การเรียกค่าไถ่ผ่าน Ransomware



3. องค์กรบางแห่งอาจใช้การโจมตีทางไซเบอร์เพื่อโมยความลับทางการค้า หรือข้อมูลที่เป็นประโยชน์ทางการแข่งขัน



4. บางประเทศอาจใช้การโจมตีทางไซเบอร์เพื่อแทรกแซงการเมือง โดยขโมยข้อมูลของหน่วยงานสำคัญ ที่ส่งผลกระทบระดับประเทศ

5. ซอฟต์แวร์และฮาร์ดแวร์ที่มีช่องโหว่ทำให้ผู้โจมตีสามารถเจาะระบบได้



6. ผู้ใช้หலายคนอาจไม่มีความรู้เกี่ยวกับความปลอดภัยไซเบอร์ทำให้พวกราดเป็นเป้าหมายที่ง่ายต่อการโจมตี

7. การเติบโตอย่างรวดเร็วของเทคโนโลยีทำให้เกิดช่องโหว่ใหม่ ๆ ที่ผู้โจมตีสามารถใช้ประโยชน์ได้



EXAMPLE

สายชอปต้องระวัง ! ตัวอย่างภัยออนไลน์ กับมาพร้อมกับ ONLINE SHOPPING

- พิชชิงและการหลอกลวง : การหลอกลวงผ่านอีเมลหรือเว็บไซต์ปลอมที่ดูเหมือนจริงเพื่อขอข้อมูลส่วนบุคคลหรือข้อมูลบัตรเครดิต
- เว็บไซต์ปลอมหรือไม่น่าเชื่อถือ
- การโจมตีแบบ Man-in-the-Middle (MitM) : ผู้โจมตีสามารถดักจับหรือแทรกแซงข้อมูลระหว่างผู้ซื้อและเว็บไซต์ โดยเฉพาะเมื่อใช้งานผ่าน Wi-Fi สาธารณะ

EXAMPLE

- มัลแวร์และไวรัส : การคลิกลิงก์หรือดาวน์โหลดไฟล์จากเว็บไซต์ไม่ปลอดภัย อาจนำไปสู่การติดตั้งมัลแวร์บนอุปกรณ์
- เว็บไซต์บางแห่งอาจเก็บข้อมูลส่วนบุคคลมากกว่าที่จำเป็น ซึ่งอาจนำไปสู่ความเสี่ยงหากข้อมูลนั้นถูกขโมย

ทุกวันนี้การซื้อของออนไลน์ แทบจะกลายเป็นส่วนหนึ่งในชีวิตประจำวัน ของเรามาไปแล้ว แต่ก็ต้องให้ระวังภัยร้ายที่อาจซ่อนอยู่ในรูปแบบของการขายสินค้าเหล่านี้ด้วย ก่อนการสั่งซื้อของออนไลน์ทุกครั้ง ต้องพิจารณา ความน่าเชื่อถือของร้าน เพื่อป้องกันการถูกฟิชชิ่ง ที่หลอกให้เรากรอก ข้อมูลส่วนตัวหรือข้อมูลบัตรเครดิตลงไป และถ้าหากว่าสักว่าร้านให้กรอก ข้อมูลเกินความจำเป็น ให้หยุดการกรอกข้อมูลทั้งหมดทันที ไม่เช่นนั้น อาจจะถูกดูดเงินได้

หรือบางครั้งอาจได้ของไม่ตรงปก ผิดสี ผิดขนาด ไม่เป็นอย่างที่คิดไว้ จะเคลมหรือร้องเรียนก็ไม่สามารถติดต่อร้านได้

หากเกิดเหตุการณ์แบบนี้ขึ้น ให้ถ่ายคลิปเป็นหลักฐานและร้องเรียนไป ทางเว็บไซต์ <https://complaint.ocpb.go.th/> หรือสายด่วน 1166 ของสำนักงานคณะกรรมการคุ้มครองผู้บริโภคได้

แหล่งข้อมูลเพื่อติดตามสถานการณ์

กิจกรรมไซเบอร์

ในประเทศไทย มีหลายหน่วยงานที่ให้ข้อมูลและอัปเดตเกี่ยวกับสถานการณ์กิจกรรมทางไซเบอร์ ซึ่งรวมถึงการแจ้งเตือน การวิเคราะห์ และคำแนะนำเกี่ยวกับวิธีป้องกันแหล่งข้อมูลเหล่านี้ เป็นทรัพยากรที่ดีสำหรับองค์กรและบุคคลในภาคธุรกิจ รวมไปถึงประชาชนทั่วไปที่ต้องการรักษาความปลอดภัยในโลกไซเบอร์ เช่น

- **ไทยเชิร์ต (THAICERT)**

หน่วยงานรับผิดชอบ ด้านการตอบสนองเหตุการณ์คอมพิวเตอร์ฉุกเฉินของประเทศไทย ให้ข้อมูลและการแจ้งเตือน เกี่ยวกับกิจกรรมทางไซเบอร์ รวมถึง มีบทความและคำแนะนำเกี่ยวกับการป้องกัน

- **สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) (National Cyber Security Agency - NCSA)**

หน่วยงานที่รับผิดชอบในการกำหนดนโยบายและแผนงานเพื่อเสริมสร้างความมั่นคงไซเบอร์ของประเทศไทย รวมทั้ง การติดตาม ประเมินกิจกรรม และตอบสนองเพื่อรับมือกับกิจกรรมทางไซเบอร์

- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
(สพธอ.) (Electronic Transactions Development Agency - ETDA)

มีบทบาทในการกำกับดูแลธุรกิจบริการดิจิทัล ควบคู่ไปกับการส่งเสริมและพัฒนาการทำธุรกรรมอิเล็กทรอนิกส์ในประเทศไทย อย่างมั่นคงปลอดภัย

- กองบัญชาการตำรวจน้ำสืบสวนสอบสวน
อาชญากรรมทางเทคโนโลยี
(บช.สอท.) หรือเป็นที่รู้จักในชื่อ "กองบัญชาการตำรวจน้ำไซเบอร์"

เป็นหน่วยงานหลักในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยีที่มีผลกระทบต่อประชาชน

- เว็บไซต์และบล็อกด้านความปลอดภัยไซเบอร์

มีเว็บไซต์และบล็อกหลายแห่ง ที่ให้ข้อมูลอัปเดตเกี่ยวกับภัยคุกคามทางไซเบอร์และการป้องกัน ซึ่งเป็นทรัพยากรที่ดีสำหรับผู้ที่สนใจเรื่องความปลอดภัยไซเบอร์

การติดตามแหล่งข้อมูลเหล่านี้ช่วยให้ผู้คนและองค์กรต่าง ๆ สามารถอัปเดตตัวเองกับข้อมูลล่าสุดเกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกัน ช่วยให้สามารถรักษาความปลอดภัยของข้อมูลและระบบของตนได้



อ่อนไลน์อย่างไร

ให้ปลอดภัย ?



TIP

การใช้อินเทอร์เน็ต และแพลตฟอร์มออนไลน์อย่างปลอดภัย เป็นสิ่งสำคัญในยุคดิจิทัล เพื่อป้องกันตัวเองจากภัยคุกคามทางไซเบอร์ และรักษาความเป็นส่วนตัว โดยมีคำแนะนำพื้นฐาน เกี่ยวกับวิธีการใช้อินเทอร์เน็ตอย่างปลอดภัย ดังนี้



1

สร้างรหัสผ่านที่ยากต่อการทาย

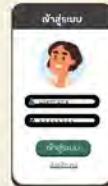
โดยควรตั้ง Password ให้ปลอดภัย ด้วยคอนเซ็ปต์ “**ไม่ซ้ำ ไม่ง่าย ไม่บอกรหัส**”

- 1) รหัสผ่านควรมีความยาวอย่างน้อย 8 ตัวอักษร
- 2) ใช้ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษ ผสมกัน
- 3) อย่าใช้ข้อมูลส่วนบุคคล เช่น วันเกิด ชื่อสัตว์เลี้ยง หรือนามสกุล
- 4) ไม่ใช้คำที่มีในพจนานุกรม
- 5) อย่าใช้รหัสผ่านเดียวกันกับหลายบัญชี
- 6) ใช้โปรแกรมจัดการรหัสผ่านที่ซับซ้อนเพื่อสร้างและเก็บรหัสผ่าน
- 7) เปลี่ยนรหัสผ่านเป็นระยะ หรือถ้ารู้สึกว่าถูกแฮกให้เปลี่ยนรหัสผ่านทันที

**TIP****2**

ใช้การตรวจสอบสองชั้นตอน

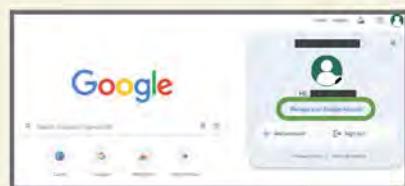
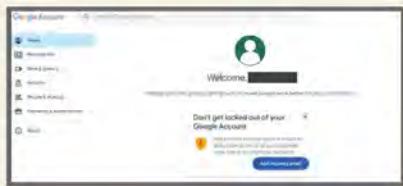
(Two-Factor Authentication: 2FA)

**ขั้นตอนที่ 1**

กดที่ภาพโปรไฟล์มุมบนขวา

**ขั้นตอนที่ 2**

กด จัดการบัญชี Google

**ขั้นตอนที่ 3**เลือกตัวเลือก ความปลอดภัย
จากเมนูด้านซ้าย**ขั้นตอนที่ 4**เลือก การยืนยันตัวตน
แบบสองชั้นตอน



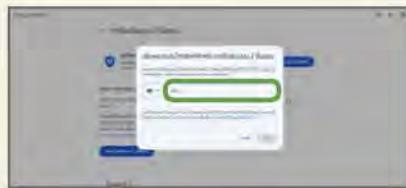
ขั้นตอนที่ 5

กด เริ่มต้นใช้งาน และใส่รหัสผ่านบัญชี จากนั้นกด ถัดไป



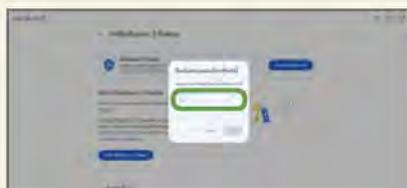
ขั้นตอนที่ 6

กรอก เบอร์โทรศัพท์ เพื่อยืนยันตัวตน



ขั้นตอนที่ 7

ใส่รหัสที่ส่งเข้ามาจากเบอร์มือถือ



ขั้นตอนที่ 8

กด เปิด เพื่อทำการเปิดการยืนยันตัวตน 2 ขั้นตอน



TIP

ในปัจจุบันมีการพัฒนามาตรฐานใหม่ขึ้นมาทดแทนการยืนยันตัวตนด้วยรหัสผ่าน (Password) สิ่งนี้เรียกว่า **Passkey**

Passkey

เป็นระบบการยืนยันตัวตนโดยไม่ใช้รหัสผ่าน แต่ใช้ระบบหลังบ้านของผู้ให้บริการในการดำเนินตามขั้นตอนทางเทคนิค ก่อนจะให้ผู้ใช้ยืนยันตัวตนด้วยการชีวมิติ เช่น การสแกนนิ้ว หรือสแกนใบหน้า บนอุปกรณ์ส่วนตัวของผู้ใช้

EXAMPLE**ตัวอย่างเช่น**

1

เมื่อเราต้องการจะเข้าสู่เว็บไซต์ที่เคยเป็นสมาชิก ระบบ Passkey ของเว็บไซต์นั้น จะสอบถาม ชื่อผู้ใช้ตามที่คุ้นเคย



2

แต่เมื่อเข้าสู่ขั้นตอนถัดไป เว็บไซต์จะแสดงรหัส QR Code ให้ผู้ใช้สแกนด้วยโทรศัพท์มือถือที่ลงทะเบียนไว้

EXAMPLE

3

อาจจะใช้การสแกนนิ้ว
หรือสแกนหน้าได้ทันที

- ระบบการยืนยันตัวตนด้วย Passkey นี้ จะปลอดภัยกว่าระบบอื่น ๆ เช่น ไม่ต้องกลัวรหัสผ่านหายแล้วโดยนิรนามหรือโอนคนร้ายหลอกให้ส่งเลข OTP รวมทั้ง ผู้ให้บริการก็ไม่ต้องกังวลว่า ข้อมูลรหัสผ่านจะรั่วหรือถูกเจาะอีกด้วย
- ขณะนี้เริ่มมีบริษัทระดับโลกหลายแห่งเปิดให้เลือกใช้ Passkey ใน การยืนยันตัวตนแล้ว หากเป็นไปได้ แนะนำให้เรียนรู้ และลองตั้งค่า การใช้งาน เพื่อความปลอดภัยที่เข้มแข็งขึ้น



TIP**3**

ระมัดระวังการคลิกลิงก์ สแกน



หรือ ดาวน์โหลดไฟล์ อย่าไว้ใจแหล่งที่ไม่น่าเชื่อถือ

เพราะลิงก์หรือการสแกน เป็นจุดเริ่มต้นสำคัญ ที่คนร้ายมักจะใช้เพื่อพาเราเข้าไปติดกับดัก ซึ่งกับดักอาจมาในรูปแบบเว็บไซต์ปลอม หรือแอปพลิเคชันปลอม อย่างไรก็ตาม ลำพังการคลิกลิงก์หรือสแกนเพียงอย่างเดียว ไม่ได้ทำให้โดนมิจฉาชีพดูดเงินทันที แต่การเข้าไปกรอกข้อมูลส่วนตัว หรือกดดาวน์โหลดแอปพลิเคชันนอกสโตร์ ที่ไม่ผ่านการรับรองต่างหาก ที่ทำให้มิจฉาชีพได้ข้อมูลไปใช้ในการดูดเงินหรือใช้มือถือเราเองในการโอนเงินหรือข้อมูลไปให้ที่ที่เข้าต้องการ

4หมั่นอัปเดตซอฟต์แวร์
และระบบปฏิบัติการอยู่เสมอ

เพื่อป้องกันจากช่องโหว่ที่อาจถูกโจมตี

5

ระมัดระวังในการใช้ Wi-Fi สาธารณะ



หลีกเลี่ยงการทำธุรกรรมทางการเงิน หรือการเข้าถึงข้อมูลสำคัญเมื่อใช้ Wi-Fi สาธารณะ บางกรณีอาจพิจารณาใช้ VPN (Virtual Private Network) เพื่อเพิ่มความปลอดภัย

TIP**6**

ตรวจสอบและปรับการตั้งค่าความเป็นส่วนตัว

**7**

ระมัดระวังการแชร์ข้อมูลส่วนบุคคล



เช่น ที่อยู่บ้าน วันเกิด หรือหมายเลขประจำตัวประชาชนในอินเทอร์เน็ต

8

สำรองข้อมูลอยู่เสมอ



ในอุปกรณ์ที่ไม่ได้เชื่อมต่อกับเครื่องคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ

9

หมั่นอัปเดตสถานการณ์



เพื่อสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ล่าสุดและวิธีการป้องกัน



หากถามถึงความเสี่ยงโลกไซเบอร์
 อาจเจอะเจอสารพัดภัยให้ปวดหัว
 มาหากลายรูปแบบพาตีนกลัว
 หมายหมองมัวล่วงละเมิดแก่กลังก่อโกร
 ทั้งยังมีภัยคุกคามล่อลงหลอก
 กลึงกลับกลอกออกอุบَاي ใจผันผวน
 ไม่ประมาทตั้งรหัสให้ครบถ้วน
 กันปั่นป่วนใช้สองขันยันพาสคีย์



ถ้าคุณเรียนผ่านด้านนี้
คุณจะเป็นส่วนหนึ่ง
ที่ช่วยให้องค์กรไม่ตกอยู่
ในความเสี่ยงจากการโจรตี
ทางไซเบอร์ ได้

3.2

ORGANIZATIONAL CYBER-RISK MANAGEMENT

วัตถุประสงค์

- ผู้เรียนสามารถเข้าใจถึงการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น และความตระหนักในภัยคุกคามได้
- ผู้เรียนสามารถเข้าใจถึงการป้องกันหรือการจัดการภัยคุกคามทางไซเบอร์ได้



First Jobber

ควรรู้ไว้ !



ถ้าคุณเป็นคนที่กำลังจะก้าวเข้าสู่การทำงานอย่างเต็มตัว คุณควรรู้ไว้ว่า การบริหารความเสี่ยงมีความสำคัญอย่างยิ่งต่อความสำเร็จ และความยั่งยืนขององค์กร ซึ่งเราควรรู้ไว้ก่อนจะสมัครงานบริษัทนั้น เพื่อให้เราเข้าใจพื้นฐานของแนวความคิดในการจัดการความเสี่ยงขององค์กร





ความเสี่ยงจากการใช้เทคโนโลยีในองค์กร



ความเสี่ยงในระดับองค์กรถือเป็นสิ่งที่จะต้องมีการจัดการอย่างรอบคอบ โดยความเสี่ยงหลัก ๆ จากการใช้เทคโนโลยีในองค์กร มีดังนี้

1

ความเสี่ยงด้านความปลอดภัย
จากการโจมตีทางไซเบอร์



สามารถทำให้องค์กรสูญเสียข้อมูลสำคัญ การเข้าถึงระบบลูกขัดของ หรือเกิดความเสียหายต่อระบบ IT ได้

2

การรั่วไหล หรือการสูญหาย
ของข้อมูลลับ และข้อมูลส่วนบุคคล



สามารถนำไปสู่ความเสียหายทางกฎหมาย ความสูญเสียทางการเงิน และความเสียหายต่อชื่อเสียงได้

3

การขาดความมั่นคง
และความพร้อมในการใช้งานของระบบ IT



สามารถนำไปสู่การหยุดชะงักของการดำเนินงาน ความล่าช้า และความเสียหายต่อการดำเนินงานขององค์กร

**WARNING****4**

ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมายและข้อกำหนด



เช่น กฎหมาย PDPA สามารถนำไปสู่ความรับผิดทางกฎหมาย และทำให้ชื่อเสียงเสียหายได้

5

ความเสี่ยงจากการใช้งานเทคโนโลยีส่วนบุคคลในการทำงาน (Bring Your Own Device)



การใช้อุปกรณ์ส่วนบุคคล สำหรับการทำงาน สามารถเพิ่มความเสี่ยงจากการรั่วไหลของข้อมูล และการโจมตีทางไซเบอร์

6

การขาดการฝึกอบรม และความตระหนักรู้ของพนักงาน



หากพนักงานขาดการฝึกอบรมเกี่ยวกับความปลอดภัยไซเบอร์ อาจทำให้เกิดความเสี่ยงจากการคลิกลิงก์ที่เป็นอันตราย หรือการเปิดเผยข้อมูลโดยไม่ระมัดระวัง

7

ความเสี่ยงจากการพึงพาผู้ให้บริการภายนอก



เช่น การพึงพาซอฟต์แวร์ บริการคลาวด์ หรือผู้ให้บริการ IT ภายนอก อาจเพิ่มความเสี่ยง หากไม่มีการจัดการ และการตรวจสอบที่เหมาะสม

EXAMPLE

WORLD ECONOMIC FORUM (WEF)

ได้มีการเผยแพร่รายงานความเสี่ยงโลกปี 2024 หรือ Global Risk Report 2024 พบว่า 10 อันดับแรกของภัยความเสี่ยงโลกตั้งแต่ปี 2024 เป็นต้นไป มีปัจจัยความเสี่ยงที่เกิดจากเทคโนโลยีเข้ามาเพิ่มเติมหลายปัจจัย ที่สำคัญ คือ

- ข้อมูลเท็จ (Misinformation)
- ข้อมูลบิดเบือน (Disinformation)

ถือเป็นความเสี่ยงที่มีแนวโน้มในการสร้างผลกระทบต่อเนื่อง ไปอีก 10 ปี ข้างหน้า เพราะการเข้าถึง AI Models ได้อย่างง่ายดาย กลยุทธ์เป็นตัวเร่งให้ ข้อมูลสังเคราะห์หรือข้อมูลเทียม จากเทคโนโลยี AI หรือ Synthetic Content กระจายไปได้อย่างรวดเร็ว สามารถเข้าแทรกแซงทำลายระบบเศรษฐกิจ ทำให้สังคมเกิดความแตกแยก เกิดความไม่ไว้วางใจในแหล่งข้อมูล ทั้งจากสื่อและภาครัฐ เหล่าโซเชียลมีเดียแพลตฟอร์มต่าง ๆ จะพบกับความยากลำบากในการนำเสนอข้อมูลที่น่าเชื่อถือ

นอกจากนี้ ยังมีภัยที่จะเกิดจากเทคโนโลยี AI ที่จะกลยุทธ์เป็นปัจจัยเสี่ยงติด TOP 10 ในอีก 10 ปีข้างหน้าด้วยเช่นกัน



รูปแบบความเสี่ยงภัยไซเบอร์ต่อองค์กร

เช่นเดียวกับภัยไซเบอร์ระดับส่วนตัว คือ แบ่งออกได้เป็น 2 เทคนิคใหญ่ คือ กลยุทธ์ทางวิศวกรรมสังคม (Social Engineering) และ การโจมตีทางเทคนิค (Technical Attacks)

การโจมตีต่อองค์กร ผู้โจมตีมีเป้าหมายสำคัญ เช่น
เงินและทรัพย์สิน หรือสิ่งที่เปลี่ยนเป็นเงินได้
เป็นหนึ่งในสาเหตุหลักของการโจมตีทั้งปวง

ข้อมูล

อาจเพื่อจารกรรมข้อมูลเพื่อนำไปขายต่อ หรือด้วยวัตถุประสงค์อื่น ๆ เช่น ฐานข้อมูลผู้ใช้ไฟล์เนื้อหาที่เป็นความลับ

ทำลายชื่อเสียง

อาจเป็นการโจมตี เพื่อให้องค์กรเป้าหมายเสียชื่อเสียง

อุดมการณ์

หล่ายครั้งผู้โจมตีอ้างเหตุอุดมการณ์ อย่างไรก็ตาม ก็มีความเป็นไปได้ว่าจะมีเรื่องอื่น ๆ เป็นสาเหตุร่วมด้วย

กลยุทธ์ทางวิศวกรรมสังคม (Social Engineering)

อีเมลหลอกให้กด หลอกให้กรอก (Phishing Scams)



การส่งอีเมลปลอมแปลงเลียนแบบองค์กรภายใน เพื่อหลอกให้พนักงาน เปิดเผยข้อมูลสำคัญหรือสิทธิ์เข้าถึงระบบ

สร้างเรื่องหลอกลวง (Pretexting)



การสร้างสถานการณ์ปลอมขึ้นมาเพื่อให้เข้าถึงสถานที่หรือระบบขององค์กร เช่น ปลอมตัวเป็นพนักงานส่งของหลอกลวงเจ้าหน้าที่รักษาความปลอดภัย

ปลอมตัวเป็นคนกลาง (Man-in-the-Middle Attack)



การหลอกลวงพนักงาน ให้เปิดเผยช่องทางเข้าถึงระบบเครือข่ายของ องค์กร จากนั้นคนร้ายจะสามารถตักจับข้อมูลการสื่อสารระหว่างทาง แล้วปลอมตัวเป็นคนกลาง เพื่อหลอกลวงทั้งฝ่ายต้นทางและปลายทาง เช่น ปลอมเป็นคนกลางระหว่างการเจราชาซื้อขายสินค้าล็อตใหญ่ เพื่อ ให้ผู้ซื้อหงุดเงินไปที่คนร้าย แทนการโอนไปยังปลายทางจริง

การโจมตีทางเทคนิค (Technical Attacks)

การระดมโจมตีให้ล่ม Denial-of-Service (DoS) Attack

การระดมเรียกใช้และเข้าถึงจำนวนมาก จนเว็บไซต์หรือเซิร์ฟเวอร์ไม่สามารถให้บริการผู้ใช้งานจริงได้



การโจมตีแบบ SQL Injection

การใช้ช่องโหว่ของระบบฐานข้อมูลเพื่อแทรกโค้ดอันตราย



การโจมตีแบบ Cross-Site Scripting (XSS Attacks)

การฝังสคริปต์อันตรายไว้ในเว็บไซต์ที่ถูกต้องตามกฎหมาย เมื่อผู้ใช้เข้าชมเว็บไซต์เหล่านั้น สคริปต์อันตรายอาจทำงานและขโมยข้อมูลได้



มัลแวร์เรียกค่าไถ่ (Ransomware)

คือมัลแวร์ประเภทหนึ่ง ที่เข้ารหัสข้อมูลของเหยื่อและเรียกร้องค่าไถ่เพื่อถอดรหัส สิ่งนี้สามารถส่งผลร้ายแรงต่อองค์กรเนื่องจากสามารถหยุดชะงักการทำงานและก่อให้เกิดความสูญเสียทางการเงินอย่างมีนัยสำคัญ

แนวปฏิบัติเพื่อร่วมกันป้องกัน ภัยไซเบอร์ระดับองค์กร



นอกจากการระมัดระวังการใช้เทคโนโลยีแบบส่วนตัวแล้ว พนักงานในองค์กรยังต้องเรียนรู้การใช้เทคโนโลยีในองค์กรอย่างเหมาะสม ตามนโยบายและรู้เท่าทัน โดยจัดแบ่งแนวปฏิบัติเป็น 4 กลุ่มใหญ่ ๆ ได้แก่

1. ตระหนักระวังภัย ({{}})

- ไม่เชื่อง่าย ไม่ตกเป็นเหยื่ออุบัtyลงให้กรอก หลอกให้กดต่าง ๆ
- มีวินัยในการจัดเก็บและใช้รหัสผ่านที่แข็งแรง ใช้ระบบยืนยันตัวตนสองขั้นตอนเสมอ (หากมี)
- พิสูจน์และยืนยันตัวตนเสมอ เมื่อจำเป็นต้องมีการเปิดเผยข้อมูลสำคัญ ส่งไฟล์ หรือโอนเงิน
- ให้ความสำคัญกับการจัดการสิทธิ์การเข้าถึงไฟล์ อุปกรณ์ หรือระบบขององค์กร
- ไม่ระวังแค่ภัยบนออนไลน์ เพราะคนร้ายอาจมาในรูปแบบการบุกรุก มาเข้าถึงข้อมูลสำคัญ หรือหลอกมายกอุปกรณ์ เพื่ออาศัยเราเป็นทางผ่านในการโจมตีได้

2. เกาะติดนโยบาย



- รู้จัก เข้าใจ และปฏิบัติตามนโยบายด้านความปลอดภัยไซเบอร์ขององค์กร
- อัปเดต อัปสกิล ติดตามข่าวสาร และเข้าร่วมการอบรมเกี่ยวกับความปลอดภัยไซเบอร์ การใช้เทคโนโลยีอย่างรับผิดชอบ เพื่อสร้างความตระหนักรู้ และยกระดับทักษะในการป้องกันภัย
- เป็นทูเป็นตา รายงานเสมอ หากพบเหตุการณ์หรือกิจกรรมเสี่ยงภัยไซเบอร์ในองค์กร ไม่ว่าจะเป็นการส่งสัญญาณโจรตีจากภายนอก หรือการมองเห็นเพื่อนร่วมงานอาจเปิดช่องโหว่
- เข้าใจกฎหมายที่เกี่ยวข้อง เช่น “พ.ร.บ. คอมพิวเตอร์” “พ.ร.บ.ไซเบอร์” และ “พ.ร.บ. PDPA” รวมทั้ง “พ.ร.บ. ดิจิทัลไอดี” และ “พ.ร.บ. แพลตฟอร์ม” หากเกี่ยวข้อง

3. รักษาความปลอดภัย



- อยู่ในมาตรฐานของมาตรการรักษาความปลอดภัยไซเบอร์ขององค์กร
- เช่น ไม่แอ็บติดตั้งแอปฯ หรืออุปกรณ์โดยไม่ได้รับอนุญาต
- หมั่นอัปเดตซอฟต์แวร์ แออนตี้ไวรัส และระบบปฏิบัติการเป็นรุ่นใหม่
- ฝึกหัดการตั้งค่าความสามารถด้านการรักษาความปลอดภัยอยู่เสมอ
- ไม่ละเลยคำเตือนที่ปรากฏบนแอปฯ หรือระบบต่าง ๆ
- ใช้เว็บไซต์และแอปพลิเคชันให้ชำนาญ เพื่อไม่ตกเป็นเหยื่อของการหลอกลวง



4. พร้อมรับหากภัยมา

- คิดไว้เสมอว่า เรายังมีโอกาสโอนโجمตีได้ทุกเมื่อ และเตรียมแผนสำรอง ที่สมเหตุผล
- สำรองข้อมูล สำรองระบบ สำรองอุปกรณ์ เพื่อให้มีความ “อึดทน” หรือ Resillience แม้มีการโอนตี แต่ก็ยังไม่เสียหายหนักจนต้องหยุด กิจการ
- ใช้หลัก BACK UP 3-2-1 คือ จัดเก็บข้อมูลสำคัญอย่างน้อย 3 ชุด ให้ อยู่ในอย่างน้อย 2 รูปแบบสื่อ (เช่น มีทั้งคลาวด์ และในฮาร์ดดิสก์) และมีอย่างน้อย 1 ชุด จัดเก็บอยู่คนละพื้นที่





TIP

Update ประเด็นความปลอดภัยทางไซเบอร์



ที่ก່ຽວโลกให้ความสำคัญ

เทคโนโลยี AI ได้มีการพูดถึงในการประชุมหลาย ๆ เวที จากระดับนานาชาติ ซึ่งหลายประเทศต่างให้ความสำคัญ รวมถึงประเทศไทย และเริ่มมีความกังวลว่าอาจมีความเสี่ยงเกิดขึ้นได้ในอนาคต เนื่องจาก การพัฒนาทางเทคโนโลยีอย่างรวดเร็ว และยังเชื่อมโยงกับเทคโนโลยี เกิดใหม่อื่น ๆ ในบางประเทศ ได้เริ่มออกมาตรการเข้มด้านความปลอดภัย ยกตัวอย่าง สหรัฐอเมริกา ที่ได้เริ่มมีแนวทางเกี่ยวกับ การใช้ AI ที่ครอบคลุมเรื่อง มาตรฐานใหม่สำหรับความปลอดภัย (AI Safety and Security) การปกป้องความเป็นส่วนตัวของพลเมือง ความเท่าเทียมและสิทธิพลเมือง ส่งเสริมสวัตกรรมและการแข่งขัน รวมถึงหน่วยงานภาครัฐใช้งาน AI ที่ใช้อย่างมีความรับผิดชอบและ มีประสิทธิภาพ เช่น

บริษัทด้าน AI ที่มีการพัฒนาและจะส่งผลกระทบต่อความมั่นคงของชาติ เศรษฐกิจ หรือความมั่นคงด้านสุขภาพจะต้องรายงานต่อรัฐบาล กำหนดให้มีการใส่ลายน้ำ (Watermark) สำหรับคอนเทนต์ที่สร้าง จาก AI เป็นต้น



กฎหมายกีดกันข้อบังคับความปลอดภัยไซเบอร์ในประเทศไทย



ในประเทศไทยมีกฎหมายกีดกันความปลอดภัยไซเบอร์ เพื่อควบคุม และป้องกันการกระทำที่ไม่เหมาะสมทางไซเบอร์ รวมถึง การปกป้อง ข้อมูลส่วนบุคคลและรักษาความมั่งคงของข้อมูล คือ

พระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 2560

โดยมีมาตราที่เกี่ยวข้อง ดังนี้

มาตรา 9 - 10

แก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหายโดยมิชอบ

จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท

หรือทั้งจำทั้งปรับ

มาตรา 11

ส่งข้อมูลหรืออีเมลก่อความผิดสื่อ หรือการส่งข้อความ

ฝากร้าน โดยที่ไม่ได้รับอนุญาต

- ส่งโดยปกปิดหรือปลอมแปลงแหล่งที่มา: ปรับไม่เกิน 1 แสนบาท

- ส่งโดยไม่เปิดโอกาสให้ปฏิเสธโดยง่าย: โทษจำคุกไม่เกิน 2 ปี

ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ

มาตรา 14

การโพสต์ข้อมูลปลอม ทุจริต หลอกลวง ข้อมูลความผิดเกี่ยวกับ ความมั่งคง ข้อมูลลามก หรือ ส่งต่อข้อมูลที่รู้อยู่แล้วว่าผิด

- หากเป็นการกระทำที่ส่งผลถึงประชาชน:

ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ

- หากเป็นกรณีที่เป็นการกระทำที่ส่งผลต่อบุคคลใดบุคคลหนึ่ง:

โทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ





สิ่งสำคัญเมื่อก้าวสู่การทำงาน

ควรเข้าใจบริหารรับความเสี่ยง

หากเพลี่ยงพล้ำข้อมูลลับสูญหายเกลี้ยง

องค์กรเสียชื่อเสียงสูญเงินตรา

เมื่อใช้ต้องป้องกันไม่ประมาท

เพื่อพลังพลาดมีแผนรับกับปัญหา

ใส่ใจทุกนโยบายล้วนมีค่า

ควรรักษา_rับผิดชอบครอบครอง

3.1

**Behavioral
Cyber-Risk Management**

ความปลอดภัย
เรื่มที่การปักป้อง
“ส่วนบุคคล”

การล่วงละเมิดทางไซเบอร์

การคุกคามทางไซเบอร์

การล่วงละเมิดทางไซเบอร์
(Cyber Abuse)

รูปแบบการล่วงละเมิด
ทางไซเบอร์

การคุกคามทางอิเล็กทรอนิกส์
(Cyberstalking)

การเปิดเผยข้อมูลส่วนตัว
(Doxing)

การกลั่นแกล้งทางไซเบอร์
(Cyberbullying)

การใช้คำพูดเกลียดชัง
(Hate Speech)

สาเหตุของการล่วงละเมิด
ทางไซเบอร์

รับมือการคุกคาม
ทางไซเบอร์

ออนไลน์อย่างไร
ให้ปลอดภัย ?

สร้างรหัสผ่าน
ที่ยากต่อการทาย

ใช้การตรวจสอบสิทธิ์
2 ขั้นตอน

Passkey

ภัยคุกคาม
ทางไซเบอร์
(Cyber Threat)

รูปแบบภัยคุกคาม
ทางไซเบอร์
ในระดับส่วนตัว

กลยุทธ์
ทางวิศวกรรมสังคม

กลยุทธ์การใจมี
ทางเทคโนโลยี

สาเหตุภัยคุกคาม
ทางไซเบอร์

แหล่งข้อมูลเพื่อติดตาม
สถานการณ์
ภัยคุกคามไซเบอร์

Organizational Cyber-Risk Management

3.2

ความเสี่ยงจากการใช้เทคโนโลยีในองค์กร

- ความเสี่ยงด้านความปลอดภัย
- การรั่วไหลของข้อมูล
- การขาดความมั่นคงของ IT
- ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมาย
- ความเสี่ยงจากการใช้งานเทคโนโลยีส่วนบุคคล
- การขาดการฝึกอบรม
- ความเสี่ยงจากการพึงพาผู้ให้บริการภายนอก

รูปแบบความเสี่ยงกับไซเบอร์ต่อองค์กร

- กลยุทธ์ทางวิศวกรรมสังคม
- การโจมตีทางเทคนิค

กฎหมายที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ในประเทศไทย

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 2560

แนวปฏิบัติเพื่อร่วมกันป้องกันภัยไซเบอร์ระดับองค์กร

จัดแบ่งแนวปฏิบัติเป็น 4 กลุ่มใหญ่ ๆ

- ตระหนักระรังษัย
- เกาดติดนโยบาย
- รักภูมิคุ้มค่าทางเทคนิค
- พร้อมรับหากภัยมา

Update ประจำเดือนความปลอดภัยทางไซเบอร์ที่ทั่วโลกให้ความสำคัญ

มาตรฐาน 9 - 10
แก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหายโดยมิชอบ

มาตรฐาน 11
ส่งข้อมูลหรืออีเมลก่อความผู้อื่นหรือการส่งข้อความ偽กันร้านโดยที่ไม่ได้รับอนุญาต

มาตรฐาน 14
การโพสต์ข้อมูลปลอม ทุจริตหลอกลวง ข้อมูลความผิดเกี่ยวกับความมั่งคง ข้อมูลตามก หรือส่งต่อข้อมูลที่รู้อย่างล้าภัย

04



การสื่อสารดิจิทัล

—Digital Communication—

ແນະນຳສໍາຮັບຜູ້ສວນ



- **ວັດຖຸປະສົງຄ່າ**

ຜູ້ເຮືອນມີຄວາມຮູ້ເກີຍກັບການສື່ອສາງໃນໂລກດິຈິທັລ ສິທອິດິຈິທັລ ແລະ ປັຈຍີທີຈະ
ທຳໃຫ້ການສື່ອສາງຫຼືການສ້າງຄວາມຮູ້ມື່ມີສໍາເຮົາ ທີ່ອລິ້ນເໝວໄດ້

- **ຂອບເຂດຂອງເນື່ອຫາດ້ານນີ້**

4.1 Digital Footprint Management

- ຄວາມໝາຍແລະການເກີດຂຶ້ນຂອງ Digital Footprint ວັນທີສອນ
...../...../.....
- ເຄື່ອງມື່ອໃນການຈັດການ Digital Footprint ວັນທີສອນ
...../...../.....
- ຮ່ອງຮອຍດິຈິທັລເຊີງບວກແລະເຊີງລົບ ວັນທີສອນ
...../...../.....
- 12 ແຫຼຸຜລີ່ Digital Footprint ດີວ່າສິ່ງສໍາຄັງຕ່ອງ HR ວັນທີສອນ
...../...../.....
- ເປີດສົດຕິ Digital Footprint ດີວ່າໜີ້ໃນແຫຼຸຜລກາຮັບພັກງານໃໝ່
ວັນທີສອນ
...../...../.....

4.2 Interaction & Collaboration

- ສິ່ງທີ່ທຳໃຫ້ການສື່ອສາງດິຈິທັລປະສົບຄວາມສໍາເຮົາ ວັນທີສອນ
...../...../.....
- ການເລືອກໃໝ່ເທິນໂລຍີເພື່ອການສື່ອສາງຍ່າງສ້າງສຽງ ວັນທີສອນ
...../...../.....
- ປັຈຍີທີທຳໃຫ້ການສື່ອສາງປະສົບຄວາມສໍາເຮົາທີ່ອລິ້ນເໝວໄດ້ ວັນທີສອນ
...../...../.....
- ການຮັບມື່ອກັບປະເທົ່ານີ້ສື່ອສາງທາງລົບ ວັນທີສອນ
...../...../.....

4.3 Future Skill สำหรับการสื่อสาร

-  ทักษะสำคัญแห่งยุคดิจิทัล วันที่สอน
_____ / _____ / _____
-  นารายาทในโลกดิจิทัล (Netiquette) วันที่สอน
_____ / _____ / _____
-  สิ่งควรปฏิบัติในการสื่อสารบนโลกดิจิทัล วันที่สอน
_____ / _____ / _____
-  สิ่งที่ควร และไม่ควรทำในโลกดิจิทัล วันที่สอน
_____ / _____ / _____

4.4 การกลั่นแกล้งทางไซเบอร์ (Cyberbully)

-  สิทธิดิจิทัล หรือ Digital Rights วันที่สอน
_____ / _____ / _____
-  Cyberbullying (การกลั่นแกล้งทางไซเบอร์) วันที่สอน
_____ / _____ / _____
-  การจัดการกับ Cyberbully วันที่สอน
_____ / _____ / _____
-  วิธีการรับมือกับการกลั่นแกล้งทางไซเบอร์ วันที่สอน
_____ / _____ / _____

เวลาในการเรียน

รู้ศัพท์ ไม่สับสน



1



COOKIES

คือ ข้อมูลขนาดเล็กที่ได้มาจากการเชื่อมต่อ
ระหว่างเว็บไซต์ กับเครื่องคอมพิวเตอร์

มีชื่อเต็มคือ HTTP COOKIE
บังก์เรียกว่า เว็บคุกี้ (WEB COOKIE)

2



VPN

เครือข่ายล่วงตัวเสมือน
(VIRTUAL PRIVATE NETWORK)

คือ เป็นกลไกสำหรับการสร้างการเชื่อมต่อ
ที่ปลอดภัยระหว่างอุปกรณ์
คอมพิวเตอร์กับอินเทอร์เน็ต

3



CRISIS

CRISIS MANAGEMENT

คือ กระบวนการที่องค์กรใช้มีประสน
เหตุการณ์ที่ไม่คาดคิดมาก่อน
เป็นปัญหาที่จำเป็นต้องแก้ไขโดยด่วน
 เพราะเป็นอันตรายต่องค์กร พนักงาน
 และผู้มีผลประโยชน์กับองค์กร

4



NETIQUETTE

มารยาทเน็ต
มาจักคำว่า NETWORK ETIQUETTE

คือ กิจกรรมการที่พึงประพฤติปฏิบัติ
ในการอยู่ร่วมกันอย่างสันติในสังคมออนไลน์
 กล่าวอีกนัยหนึ่งคือ ชุดวิธีประพฤติตน
 ที่เหมาะสม เมื่อคุณใช้อินเทอร์เน็ต

รู้ศัพท์ ไม่สับสน



5



DIGITAL RIGHTS

สิทธิดิจิทัล

คือ สิทธิมนุษยชน และสิทธิ์ตามกฎหมาย
ที่อนุญาให้บุคคลเข้าถึง ใช้สร้างและเผยแพร่
สื่อดิจิทัล หรือเข้าถึงและใช้คอมพิวเตอร์อุปกรณ์
อิเล็กทรอนิกส์อื่น ๆ และเครื่องช่วยโทรศัมนาคม

6

DIGITAL HARASSMENT

คือ การกระทำใด ๆ ในช่องทาง
การสื่อสารดิจิทัลที่เกี่ยวข้องกับ
เรื่องทางเพศต่อบุคคลอื่นที่เข้ารับรู้ได้ว่า
ลงทะเบียน ไม่ต้องการ ไม่อินยอม ไม่พร้อม
หรือแม้แต่ยินยอมในขั้นตอนนั้น
แต่หากส่งผลกระทบเป็นลบต่อผู้ถูกกระทำ
คือว่าเป็นการคุกคามทางเพศได้

7

DIGITAL RESILIENCE

ภูมิคุ้มกันในโลกดิจิทัล

คือ กระบวนการต้านการปรับตัวทางบวก
และลดผลกระทบทางลบต่อชีวิตตนเอง
เมื่อต้องเผชิญกับความไม่ปลอดภัย
บนโลกออนไลน์



ถ้าคุณเรียนผ่านด้านนี้
คุณจะไม่เสียเงินไว้ลือก
เมื่อันพนักงานกว่า 34 %
ที่ใช้โซเชียลมีเดียไม่เหมาะสม*

* การสำรวจระดับประเทศได้ดำเนินการออนไลน์ในนามของ CareerBuilder โดย The Harris Poll ระหว่างวันที่ 4 เมษายนถึง 1 พฤษภาคม 2018 โดยมีกลุ่มตัวอย่างที่เป็นตัวแทนผู้จัดการการจ้างงาน และผู้เชี่ยวชาญด้านทรัพยากรบุคคลมากกว่า 1,000 ราย จากอุตสาหกรรมและขนาดบริษัทในภาคเอกชน

อ้างอิงข้อมูลจาก

<https://press.careerbuilder.com/2018-08-09-More-Than-Half-of-Employers-Have-Found-Content-on-Social-Media-That-Caused-Them-NOT-to-Hire-a-Candidate-According-to-Recent-CareerBuilder-Survey>

4.1

DIGITAL FOOTPRINT MANAGEMENT

วัตถุประสงค์

- ผู้เรียนสามารถเข้าใจถึง DIGITAL FOOTPRINT และผลกระทบที่เกิดขึ้น
- ผู้เรียนสามารถเข้าใจถึงการจัดการและความตระหนักรักกับ DIGITAL FOOTPRINT ได้

ร่องรอยการสื่อสาร ที่เราต่างกิ่งไว



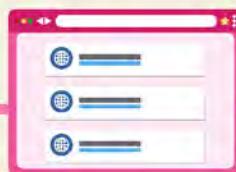
การสื่อสารดิจิทัล (Digital Communication)

หมายถึง การสื่อสารข้อมูล ตลอดจนความคิดเห็นผ่านช่องทางดิจิทัล ซึ่งจะรวมถึงสื่อสังคมออนไลน์ อีเมล เว็บไซต์ โทรศัพท์มือถือ วิดีโอดอกол เกมออนไลน์ และอื่น ๆ อีกมากมาย

และทุกครั้งที่เราสื่อสารผ่านทางดิจิทัล ไม่ว่าจะเป็นการโพสต์ข้อความ แสดงความคิดเห็น แชร์รูปภาพ หรือวิดีโอ ล้วนทิ้งร่องรอยข้อมูลของเราวัยบนโลกออนไลน์ด้วย ซึ่งร่องรอยเหล่านี้เรียกว่า Digital Footprint

Digital Footprint หรือที่เรียกว่า “ร่องรอยดิจิทัล”

หากเปรียบกับการกระทำของเรานาในโลกความจริงแล้ว ก็เหมือนกับการที่เราไปในสถานที่ต่าง ๆ เมื่อเราเดินผ่านก็จะเกิดรอยเท้า หรือถ้าเดินผ่านใครสักคน ๆ นั้นก็อาจจะจำเราได้ และเมื่อต้องมีการติดตามตัวเรา ก็จะอาศัยร่องรอยเหล่านี้ในการติดตามตัวเราในโลกดิจิทัลเช่นกัน



ประเภทของ Digital Footprint

รอยเท้าดิจิทัลมี 2 ประเภทคือ

1. รอยเท้าดิจิทัลที่ถูกเก็บโดยอัตโนมัติจากเว็บไซต์ หรือแอปพลิเคชัน (Passive Digital Footprint)

คือร่องรอยข้อมูล ที่เราไม่ได้ตั้งใจทิ้งไว้บนโลกออนไลน์ หรือข้อมูลที่ถูกเก็บรวบรวมโดยอัตโนมัติ จากเว็บไซต์ แอปพลิเคชัน หรือบริการต่าง ๆ ที่เราใช้งาน โดยที่เราอาจไม่รู้ตัว หรือไม่ได้ตั้งใจ เช่น

- **ประวัติการเข้าชมเว็บไซต์ (Browsing History)**
บันทึกเว็บไซต์ที่เราเคยเข้าชม
- **ประวัติการค้นหา (Search History)**
บันทึกคำค้นหาที่เราเคยใช้
- **ข้อมูลการใช้งานแอปพลิเคชัน**
เช่น เวลาที่ใช้ ความถี่ในการใช้งาน
- **Cookies**

ไฟล์ขนาดเล็กที่เว็บไซต์เก็บไว้ในอุปกรณ์ของเรา เพื่อจดจำข้อมูลการใช้งาน และปรับแต่งประสบการณ์การใช้งาน



WARNING



อยากรีบเพื่อน



- **IP Address**

หมายเลขประจำตัว ของอุปกรณ์ที่เราใช้ในการเชื่อมต่ออินเทอร์เน็ต ซึ่งสามารถระบุผู้ให้บริการอินเทอร์เน็ต และตำแหน่งโดยประมาณ ของเราได้

แม้ว่ารอยเท้าดิจิทัลประเภทนี้ อาจไม่เปิดเผยข้อมูลโดยตรง แต่ก็อาจถูกนำไปใช้ในทางการตลาด หรือนำไปใช้ในทางที่ไม่ดี ดังนั้น ควรมีการตระหนักและป้องกันข้อมูล เช่น การลบประวัติการเข้าชมเว็บไซต์ และการค้นหา การปิดการใช้งาน Cookies หรือการใช้ VPN เป็นต้น

2. รอยเท้าดิจิทัลที่เราตั้งใจเผยแพร่ (Active Digital Footprint)

คือร่องรอยข้อมูลที่เราจงใจสร้าง และเผยแพร่บนโลกออนไลน์ด้วยตนเอง โดยมีเจตนาให้ผู้อื่นเห็น หรือเข้าถึงข้อมูลเหล่านี้ เช่น

- **โพสต์บนโซเชียลมีเดีย :**

ข้อความ รูปภาพ วิดีโอ ที่เราโพสต์ลงบนแพลตฟอร์มต่าง ๆ

- **ความคิดเห็นและรีวิว :**

ความคิดเห็นที่เราแสดงบนเว็บไซต์ บล็อก หรือแพลตฟอร์มต่าง ๆ

- **อีเมล :**

อีเมลที่เราส่งถึงผู้อื่น





WARNING

- **โปรไฟล์ออนไลน์ :**

ข้อมูลส่วนตัวและประวัติที่เราสร้างบนเว็บไซต์ หรือแอปพลิเคชัน

- **การสมัครสมาชิกเว็บไซต์ หรือบริการ :**

ข้อมูลที่เรากรอก เพื่อสมัครสมาชิกเว็บไซต์ หรือบริการ

การจัดการรอยเท้าดิจิทัลประเภทนี้ คือ การใช้อย่างมีสติ และรอบคอบ
เนื่องจากข้อมูลเหล่านี้ สามารถส่งผลกระทบต่อภาพลักษณ์ และชื่อเสียง
ของเราในโลกออนไลน์ได้



เครื่องมือในการจัดการ Digital Footprint

1. ตั้งค่าความเป็นส่วนตัวอย่างเข้มงวดบนโซเชียลมีเดีย

รวมทั้งช่องทางทางออนไลน์ต่าง ๆ ที่ใช้งาน และระวังในการแชร์ข้อมูลลงบนโซเชียลมีเดีย



2. ลบประวัติการค้นหาและคุกคัก (Cookie) เป็นประจำ



3. ใช้ VPN ในกรณีต้องใช้ Wi-Fi สาธารณะ



เมื่อต้องการเข้าถึงข้อมูลส่วนตัว เนื่องจาก VPN ช่วยให้บุคคลที่ 3 เข้าถึงหรือติดตามกิจกรรมออนไลน์ของเราได้ยากขึ้นและหมายเลข IP ที่แท้จริงของเราจะถูกปิดบังเอาไว้



ร่องรอยดิจิทัล เชิงบวก และเชิงลบ

1. ร่องรอยดิจิทัลเชิงบวก



เป็นร่องรอยจากพฤติกรรม ที่สร้างขึ้นบนโลกดิจิทัล โดยไม่ทำให้ผู้อื่นเดือดร้อนหรือเกิดความเสียหาย และส่งผลต่ออัตลักษณ์ดิจิทัลและการใช้งานดิจิทัลที่เป็นประโยชน์ด้วย เช่น

- โพสต์อย่างสร้างสรรค์ เป็นกลาง และชื่นชมผู้อื่นด้วยความจริงใจ และมีความระมัดระวังข้อความหรือรูปภาพที่จะทำให้คนผู้อื่นเสียหายได้
- แสดงความคิดเห็นในโพสต์หรือแชทกับผู้อื่น ด้วยข้อความที่สุภาพ นุ่มนวล ไม่ดูถูกความคิดเห็นของผู้อื่น แม้บางครั้งอาจมีความเห็นที่ขัดแย้งก็ตาม
- ค้นหาข้อมูลที่เป็นประโยชน์และสร้างสรรค์ ระบบจะเก็บประวัติการค้นหา และอาจมีการนำเสนอหาที่เกี่ยวข้องกับเรื่องนั้น ๆ อย่างโดยอัตโนมัติที่มีการใช้งานเป็นประจำ เป็นการสะสมท่อนถึงพฤติกรรมของผู้ใช้งานแต่ละคนไปด้วย

2. ร่องรอยดิจิทัลเชิงลบ



เป็นร่องรอยจากพฤติกรรมที่สร้างขึ้น แล้วอาจทำให้ผู้อื่นเดือดร้อนเสียหาย และส่งผลที่ไม่ดีต่ออัตลักษณ์ดิจิทัลของผู้ใช้งาน ไปจนถึงอาจทำให้เกิดโทษ หรือสร้างความรำคาญได้ เช่น

- โพสต์พادพิงถึงผู้อื่นในทางที่ไม่ดี เสียดสี หรือไม่ระวัง จะให้เกิดความเสียหายหรืออับอาย
- แสดงความคิดเห็นในโพสต์ของผู้อื่นด้วยข้อความที่ไม่สุภาพ หยาบคาย หรือถ้อยคำที่รุนแรง หรือสร้างความขัดแย้ง อาจทำให้เกิดการตอบโต้ หรือโต้เถียงกัน
- ค้นหาข้อมูลที่ไม่เป็นประโยชน์หรือข้อมูลที่ไม่สร้างสรรค์ เช่น การค้นหาข้อมูลเกี่ยวกับความรุนแรง เรื่องเพศ หรือข้อมูลการพนัน ซึ่งเมื่อค้นหาข้อมูลที่ไม่สร้างสรรค์เหล่านี้บ่อยครั้ง ระบบจะเก็บข้อมูลและนำเสนอข้อมูลในลักษณะเดียวกัน แม้ว่าภัยหลังเราจะไม่ได้ค้นหาหรือพูดถึงมันแล้วก็ตาม เราจะติดอยู่ใน “ฟองสบู่ช่าวสาร” (Filter Bubble) รับสารด้านเดียว จนเกิดเป็นความเชื่อผิด ๆ ได้ และบางครั้งอาจทำให้เราระวังตัวเองเป็นศูนย์กลางของทุกอย่าง หรือถ้ารับความเห็นด้านลบมาก ๆ ก็มีโอกาสที่จะตกอยู่ในความสิ้นหวังได้ด้วย

ผลกระทบในเชิงลบที่เกิดขึ้น อาจจะเป็นการละเมิดสิทธิผู้อื่น ถึงขั้นการฟ้องร้องทางกฎหมาย หรือมีผลกับการเรียนและการทำงานในอนาคต โดยร่องรอยดิจิทัลที่สร้างขึ้น สามารถที่จะนำไปเป็นหลักฐานในทางกฎหมายได้

สุดท้ายหากร่องรอยดิจิทัลของเราดูแล้วมีปัญหา มีแต่แฉลบ ทำตัวไม่ดี ก็สามารถทำให้ HR ที่เข้ามาตรวจเช็คโโซเชียลมีเดียช่วงที่สมัครงานตัดสินใจไม่จ้างงานเราได้



12 เหตุผล ที่ Digital Footprint คือสิ่งสำคัญต่อ HR



สำหรับการสมัครงานนั้น มีหลักเกณฑ์มากมายที่ HR (Human

Resource หรือ งานบริหารทรัพยากรบุคคล) ใช้ในการประเมิน ซึ่งในปัจจุบัน โลกดิจิทัลทำให้เกิดการเปลี่ยนแปลง นอกจากที่อาจดูเพียงประวัติและผลงาน ผ่าน Resume Portfolio หรือการสัมภาษณ์แล้ว ยังรวมถึง Digital Footprint ที่ HR เริ่มนำมาเป็นส่วนหนึ่งในการตัดสินใจ คัดเลือกพนักงานมากขึ้น และในขณะเดียวกัน ผู้สมัครงานก็สามารถตรวจสอบ Digital Footprint ของบริษัทที่กำลังจะสมัครงานได้ด้วย โดย Forbes (นิตยสารเกี่ยวกับธุรกิจและการเงินในสหรัฐอเมริกา) ได้กล่าวถึงเหตุผล 12 ข้อที่ Digital Footprint สำคัญต่อ HR ดังนี้

1

ข้อมูลออนไลน์สามารถบ่งบอก
ถึงความเหมาะสมสมต่อบริษัท

การจ้างงานมีผลต่อความสำเร็จขององค์กร การศึกษาข้อมูลออนไลน์ของผู้สมัคร จะทำให้ทราบคร่าว ๆ ว่า เขายังมาสมกับเป้าหมายขององค์กรหรือไม่



2 แสดงให้เห็นตัวตนอีกด้านของผู้สมัคร

การมีตัวตนในโลกออนไลน์ที่ได้เด่น น่าสนใจ ก็จะสร้างความแตกต่าง ท่ามกลางตัวเลือกมากมายได้



3 กำจัดผู้สมัครที่อาจมีปัญหาออกໄປ

เราสามารถเห็นพฤติกรรมทั้งดีและไม่ดีในโลกออนไลน์ โดยสามารถนำข้อมูลเหล่านั้นมาประเมินว่าจะส่งผลอย่างไรกับบริษัทบ้าง



4 ดูว่าการแสดงตัวตนทางอونไลน์ของผู้สมัคร

มีคุณค่ากับองค์กรหรือไม่



5 ข้อมูลอ่อนไลน์ทำให้น้องเห็นผู้สมัคร 360 องศา

เพื่อประเมินทักษะ ความสามารถ และตัวตนของผู้สมัครว่าสอดคล้องกับวัฒนธรรมองค์กรหรือไม่



6 ทบทวนฟีดแบ็ค หรือคติที่ได้รับมา

บางครั้งเรารับฟีดแบ็คที่ไม่ดีของผู้สมัครมา การเข้าไปตรวจสอบข้อมูลดิจิทัลก็จะช่วยให้เราทราบและประเมินคตินั้น ๆ ว่าเป็นจริงหรือไม่



7 สามารถประเมินบุคลิกภาพเบื้องต้น

ท่ามกลางสถานการณ์ COVID-19 ที่เผชิญหน้ากันโดยตรงอาจเป็นเรื่องยาก การเข้าไปตรวจสอบข้อมูลออนไลน์ก็จะช่วยให้ HR เห็นบุคลิกและทัศนคติคร่าว ๆ ของผู้สมัครง่ายขึ้น



8 ตรวจดูความสนใจ ว่าสอดคล้องกับบริษัทหรือไม่

ทุกวันนี้ผู้สมัครหลายคนมีบล็อกเป็นของตัวเอง หรือเราสามารถเช็คดูการมีความส่วนร่วมของเขาว่าอยู่ในกลุ่มความสนใจใด เช่น เราเป็นบริษัทขายเสื้อผ้า และผู้สมัครเขียนบล็อกเกี่ยวกับแฟชั่น ก็จะส่งผลดีต่อธุรกิจของเราได้



9 เห็นผู้สมัครในฐานะคณคนหนึ่ง

การตรวจสอบข้อมูลออนไลน์ก็จะเห็นทักษะอื่นด้วย เช่น ทักษะการสื่อสาร การเป็นผู้นำ การตัดสินใจ



10 ตัวแทนทางดิจิทัลจะบ่งบอกว่า อะไรสำคัญต่อผู้สมัคร

ไม่ว่าจะเป็นบล็อกที่เขียน บทความที่แชร์ หรือ LinkedIn เป็นเครื่องมือสำคัญในการประเมินตัวผู้สมัคร เพราะจะสะท้อนว่าอะไรอยู่ในความสนใจ มีสนใจอย่างไร และมีไลฟ์สไตล์อย่างไร



11 สร้างความชัดเจนจากการสัมภาษณ์

บางครั้งการสัมภาษณ์อาจไม่เพียงพอ การตรวจเช็คข้อมูลออนไลน์ก็จะทำให้เรื่องราวเหล่านั้นกระจุ่งชัดเจนมากขึ้น



12 เป็นสิ่งที่ควรทำ และหลีกเลี่ยงความประหลาดใจ

หลายคนชอบโพสต์โซเชียลมีเดียทุกวัน ซึ่งจะบ่งบอกว่า เขามองโลกหรือมีความคิดเห็นอย่างไร และนั่นเป็นสิ่งที่นายจ้างควรรู้



เปิดสถิตि Digital Footprint

คือหนึ่งในเหตุผล 

การรับพนักงานใหม่

อ้างอิงจากสถิติของ CareerBuilder ในปี 2018 จากผลการสำรวจเมื่อวันที่ 4 เมษายน 2018 ถึง 1 พฤษภาคม 2018 โดยผู้ว่าจ้าง และ HR มากกว่า 1,000 คน พบว่า Digital Footprint คือหนึ่งในเหตุผลที่ทำให้องค์กรตัดสินใจ ไม่รับสมัครพนักงานใหม่ หรือไล่พนักงานเดิมออก ซึ่งความน่าสนใจของผลสำรวจ คือ มีผู้จ้างงานกว่า 70% ยอมรับว่าได้ใช้โซเชียลมีเดีย ในการค้นหาข้อมูลของผู้สมัครงานระหว่างกระบวนการสรรหาบุคคล โดยสิ่งที่พิจารณาตรวจสอบก็คือ

คุณสมบัติสนับสนุนในการจ้างงาน 58%



ความเป็นมืออาชีพในโลกออนไลน์ 50%



สิ่งที่คนอินเพสต์เกี่ยวกับผู้สมัคร 34%



เหตุผลที่จะไม่รับผู้สมัคร 22%



3 อันดับ Digital Footprint ร้ายแรงที่จะไม่รับเข้าทำงาน



อันดับที่ 1 โพสต์ภาพ วิดีโอ หรือข้อมูลยั่วยุหรือไม่เหมาะสม 40%

อันดับที่ 2 โพสต์ภาพการดื่มสุราหรือใช้ยาเสพติด 36%

อันดับที่ 3 โพสต์ข้อความเหยียดเพศ เชื้อชาติ ศาสนา 31%

3 อันดับ Digital Footprint ที่เป็นประโยชน์ต่อการรับเข้าทำงาน



อันดับที่ 1 ประวัติผู้สมัครสนับสนุนต่อหน้าที่การทำงาน 37%

อันดับที่ 2 มีความคิดสร้างสรรค์ 34%

อันดับที่ 3 ตัวตนออนไลน์มีความเป็นมืออาชีพ 33%

EXAMPLE

**ยกตัวอย่างจากข่าวเรื่อง รอยเท้าดิจิทัล :
ฝ่ายบุคคลเตือน ตัวตนและความคิดเห็น
ในโลกออนไลน์มีผลต่อการสมัครงาน**



GETTY IMAGES

ดร.บวนันท์ ทองกัลยา นายกสมาคมการจัดการงานบุคคลแห่งประเทศไทย เปิดเผยกับบีบีซีไทยว่า ปัจจุบันองค์กรธุรกิจจำนวนมากใช้ข้อมูลจากโซเชียลมีเดียประกอบการพิจารณารับบุคคลเข้าทำงาน นอกจากเนื้อหาจากการสัมภาษณ์ และการทดสอบความสามารถ ดังนั้น คนในตลาดแรงงานจึงควรระมัดระวังในการเปิดเผยข้อมูลส่วนตัว และความคิดเห็นในโลกออนไลน์ เพราะอาจส่งผลกระทบต่อการสมัครงาน

"โซเชียลมีเดียเหล่านี้เก็บข้อมูลของบุคคลได้ทั้งหมด ทำให้ฝ่ายบุคคลวิเคราะห์ผู้สมัครได้ง่าย และได้ผลมากกว่าการนั่งสัมภาษณ์แบบเดิม ๆ เพราะเราจะรู้ได้ว่าเขาให้ความสำคัญกับเรื่องไหนในชีวิต ทัศนคติ วิธีบ่น วิธีคิด" ดร.บวนันท์กล่าว

แนวโน้มนี้ได้รับการยืนยัน จากการสำรวจของสมาคมการจัดการงานบุคคลฯ เรื่องกระบวนการรับสมัครงานของบริษัทเอกชน 350 แห่ง ซึ่งจัดทำเมื่อเดือนมิถุนายนปี 2019 ผลการสำรวจพบว่า 41.19 เปอร์เซ็นต์ขององค์กรที่สำรวจ ดูโซเชียลมีเดียของผู้สมัครประกอบการพิจารณาคุณสมบัติเพื่อตัดสินใจรับเข้าทำงาน





ทุกสื่อสารผ่านข้อมูลดิจิทัล
 ร่องรอยนั้นสักไว้ไม่หาย
 สร้างรอยเท้าคนเข้าดูรู้ได้ง่าย
 โพลต์แซร์ไลก์มีให้ส่องทุกช่องทาง
 เปรียบเป็นดั่งประวัติคนผลสองด้าน
 เมื่อพบท่านเห็นส่วนดีมีแบบอย่าง
 ที่ไม่ดีแม้ลับได้ไม่ควรสร้าง
 ตั้งค่าอย่างเข้มงวดเป็นส่วนตัว



ถ้าคุณเรียนผ่านด้านนี้

คุณจะมีทักษะการสื่อสารที่ดีขึ้น
ซึ่งถือเป็นทักษะสำคัญอันดับ 1

ที่นายจ้างกำลังมองหา

อ้างอิงข้อมูลจาก

<https://www.blockdit.com/posts/66544213f864a30fba993157>

4.2

INTERACTION & COLLABORATION

วัตถุประสงค์

- ผู้เรียนสามารถเลือกใช้วิธีการสื่อสารที่เหมาะสมได้
- ผู้เรียนสามารถวิเคราะห์ปัจจัยที่จะทำให้การสื่อสารหรือการสร้างความร่วมมือสำเร็จ หรือล้มเหลวได้



ทักษะพื้นฐาน สื่อสารอย่างเข้าใจ

การสื่อสารเป็นทักษะพื้นฐานสำคัญอย่างหนึ่งในการทำงาน และการดำเนินชีวิต หากเรามีการสื่อสารที่สร้างสรรค์จะช่วยให้เกิดความเข้าใจซึ่งกันและกัน ลดความขัดแย้ง มีการแลกเปลี่ยนความรู้ และทำให้การร่วมมือกันทำงานนั้นมีประสิทธิภาพ

สิ่งที่ทำให้การสื่อสารดีจัง!



เกิดจากปัจจัยหลายประการ เช่น

- ความสนใจในเรื่องที่พูด
- การเข้าถึงคนจำนวนมากผ่านการโพสต์หรือแชร์ข้อมูลผ่านแพลตฟอร์มที่ได้รับความนิยม
- การรองรับเนื้อหาในรูปแบบที่หลากหลายตามเทคโนโลยีที่ใช้งาน
- สามารถทำได้โดยไม่จำกัดสถานที่ และมีต้นทุนต่ำ

การเลือกใช้เทคโนโลยีเพื่อการสื่อสารอย่างสร้างสรรค์



การเลือกใช้เทคโนโลยีเพื่อการสื่อสารให้เหมาะสมกับกลุ่มเป้าหมาย ที่จะสื่อสารจึงเป็นสิ่งที่ต้องคิดคำนึงถึงเป็นอันดับต้น ๆ เราอาจต้องเริ่มจากพิจารณาจากความเหมาะสมของคนหรือกลุ่มคนที่เรามีปฏิสัมพันธ์ด้วย

1. การสื่อสารระหว่างบุคคล

เลือกใช้สื่อเทคโนโลยีที่เหมาะสมกับการสื่อสารแบบตัวต่อตัว และไม่มีผู้อื่นเข้ามาแทรก เช่น โทรศัพท์ หรือ การสนทนาน่า่นอนช่องทางส่วนตัว

2. การสื่อสารระหว่างกลุ่มคน เฉพาะกลุ่มแบบไม่เป็นสาธารณะ

อาจใช้วิธีการตั้งกลุ่มการสื่อสาร ที่อนุญาตเฉพาะผู้ที่มีส่วนเกี่ยวข้องถึงจะเข้าร่วมได้

3. การสื่อสารระหว่างกลุ่มคนแบบเป็นสาธารณะ

ใช้การโพสต์เป็นสาธารณะหรือตั้งกลุ่ม ซึ่งคนที่มีความสามารถเข้าร่วมกลุ่มได้อย่างอิสระ โดยไม่ต้องรอถูกเชิญเข้ากลุ่ม แต่ต้องปฏิบัติตามข้อกำหนดของกลุ่ม

ปัจจัยที่ทำให้การสื่อสาร ✅ ✖️ ประสบความสำเร็จหรือล้มเหลว

1. เครื่องมือสื่อสารดีมัชัยไปกว่าครึ่ง



เลือกเครื่องมือสื่อสารให้เหมาะสมสมกับเป้าหมายที่ต้องการสื่อสาร โดยต้องคิดถึงข้อจำกัดต่าง ๆ เช่น ปัญหาอินเทอร์เน็ต ไม่มีมือถือ หรือมีสัญญาณรบกวน รวมถึงทักษะการใช้เครื่องมือ หรือความคุ้นเคยกับช่องทางที่ใช้ทั้งในผู้ส่งและผู้รับสาร

2. เนื้อหาชัดเจน สื่อสารฉบับไว



เนื้อหาที่สื่อสาร ต้องบอกเล่าความต้องการของผู้ส่งได้ ไม่คลุมเครือ ไม่สร้างความขัดแย้ง มีที่มาที่ไป

3. เข้าใจความต่าง หนทางของผู้อยู่เป็น



เข้าใจในวัฒนธรรมและการใช้ภาษาที่แตกต่างกัน เนื่องจากเรารอยู่กับคนละที่ บางคนอาจไม่เคยพบรือกันในโลกแห่งความเป็นจริง

4. ก้าวจำดี มีมารยาท



ครรรมีมารยาทในการสื่อสาร ยิ่งถ้ามีการประชุมออนไลน์ให้พยายามรักษา มารยาทเหมือนการประชุมจริง ๆ ตัวอย่างเช่น เข้าประชุมตรงเวลา แต่งตัวให้เรียบร้อย เปิดกล้องและเปิดฟังก์ชันเบล็อกพื้นหลัง กดปุ่มยกมือ ก่อนพูดหรือเสนอความคิดเห็น รวมไปถึง การทำสภาพแวดล้อมให้ เหมาะสมกับการประชุม เช่น มีแสงที่เพียงพอ หรือแยกสัดส่วนเลี้ยงไปไว้อีก ที่หนึ่ง

5. วิเคราะห์สุดเฉียบ เพียงพร้อมด้วยแนวทาง



วิเคราะห์ และปรับแนวทางการสื่อสารให้เหมาะสมกับทัศนคติ ประสบการณ์ และความเชื่อของกลุ่มเป้าหมาย เพราะผู้คนใช้สิ่งเหล่านี้ ตีความเนื้อหาที่ได้รับรู้มาแตกต่างกันไป

6. สื่อสารอย่างเข้าใจ ดีต่อใจคุณผู้ฟัง



ผู้ส่งสารต้องเข้าใจในสิ่งที่ต้องการสื่อสารเป็นอย่างดี มีเจตนาที่ดีและเคารพ ผู้ฟัง

7. รับสารอย่างดี เพิ่มดีกรีความเข้าใจ



ผู้รับสารต้องพยายามทำความเข้าใจและตั้งใจรับฟังเนื้อหา

การรับมือกับ ประเด็นสื่อสารทางลบ

ระดับบุคคล

1. หลีกเลี่ยงการโต้ตอบทันทีที่เห็นข้อความเชิงลบ



2. ถอยออกมาประเมินสถานการณ์ให้ดีก่อนตอบพิจารณาว่ามีพื้นฐานความจริงหรือไม่ บางครั้งอาจเลือกที่จะไม่ตอบโต้หากไม่มีประโยชน์



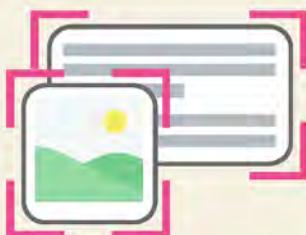
3. ใช้การตั้งค่าความเป็นส่วนตัวตามความเหมาะสมของข้อมูล



4. หากมีสถานการณ์ด้านลบเกิดขึ้นให้ปรึกษาหรือระบายกับคนที่ไว้ใจได้

5. กดรายงาน หรือบล็อกทันที หากถูกคุกคาม จนเกินขอบเขตที่ยอมรับได้

รายงาน



6. หากถูกคุกคามให้ทำการบันทึกหลักฐาน หรือแcapรูปภาพ เพื่อเป็นหลักฐานในการดำเนินการทางกฎหมาย

7. ดูแลสุขภาพจิต หากสถานการณ์ด้านลบมีผลกระทบต่อจิตใจอย่างมาก ให้ปรึกษาผู้เชี่ยวชาญด้านจิตวิทยา

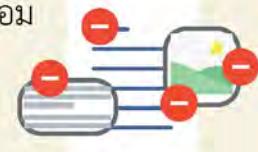


8. ใช้ประสบการณ์ต่าง ๆ ที่ได้รับไปพัฒนาปรับปรุงทักษะการสื่อสารบนโลกดิจิทัล

การรับมือกับ ประเด็นสื่อสารทางลบ

ระดับองค์กร

- เตรียมพร้อมรับมือการสื่อสารทางลบ ที่มักเกิดขึ้นได้เสมอในองค์กร สร้างการตระหนักรู้และการเตรียมพร้อม โดยการทำความเข้าใจเกี่ยวกับภัยคุกคามทางดิจิทัล และความมีอยู่บาย หรือแนวทางการจัดการที่ชัดเจน



- ตอบสนองอย่างมีอาชีพ มีเหตุผลและหลีกเลี่ยงการใช้อารมณ์
- มีแผนการจัดการวิกฤต และจัดตั้งทีมไว้สำหรับจัดการสถานการณ์วิกฤต เพื่อรับมือและรักษาภาพลักษณ์ขององค์กร ในสถานการณ์ฉุกเฉิน

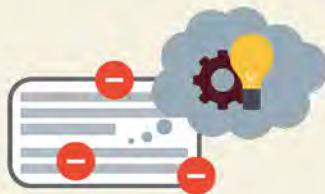


- การสื่อสารที่ตรงไปตรงมา และเป็นความจริง

5. การมีเครือข่ายพันธมิตร จะช่วยเหลือสนับสนุน
องค์กรในการจัดการสถานการณ์ต่าง ๆ ได้



6. ติดตามและวิเคราะห์สถานการณ์ด้านลบ
ที่เกิดขึ้นอย่างใกล้ชิด เพื่อหาวิธีการตอบสนอง
ที่ดีที่สุด และมีผลกระทบน้อยที่สุด



7. ศึกษา และอบรมกระบวนการเกี่ยวกับ
การสื่อสารดิจิทัลที่มีประสิทธิภาพ เช่น
Crisis Management



8. กำหนดแผนองค์กร โดยให้ความสำคัญ
กับสุขภาพจิตของบุคคลในองค์กร





ทักษะหนึ่งสำคัญขึ้นพื้นฐาน
 คือสื่อสารอย่างสร้างสรรค์เอาใจใส่
 คำนึงถึงสื่อเทคโนโลยีที่เลือกใช้
 ควรเลือกให้เหมาะสมกับบุคคล
 ปัจจัยที่การสื่อสารจะสำเร็จ
 ควรถือเคล็ดเครื่องมือดีบังเกิดผล
 เนื้อหาชัดวิเคราะห์เฉียบเข้าถึงคน
 จะรอดพ้นความล้มเหลวได้ด้วยดี



ถ้าคุณเรียนผ่านด้านนี้ คุณจะมี
ทักษะแห่งอนาคตเพิ่มขึ้น
เป็นทักษะที่นายจ้างกว่า 75%
มองว่า สำคัญมากในอนาคต*

* รายงาน Future of Jobs ประจำปี 2023 เก็บข้อมูลจากบริษัท 803 แห่ง
ซึ่งจ้างงานรวมกันกว่า 11.3 ล้านคน จาก กลุ่มอุตสาหกรรม 27 แห่ง¹
และ 45 เศรษฐกิจจากทุกภูมิภาคของโลก

อ้างอิงข้อมูลจาก

<https://www.weforum.org/publications/the-future-of-jobs-report-2023/>

4.3

FUTURE SKILL สำหรับการสื่อสาร

วัตถุประสงค์

- ผู้เรียนมีความรู้เกี่ยวกับ มารยาทในโลกดิจิทัล (NETIQUETTE) และแนวทางปฏิบัติในการส่งข้อความหรือโพสต์เพื่อสื่อสารบนโลกดิจิทัล

DO'S

DO'S





ทักษะสำคัญ แห่งยุคดิจิทัล



Future Skill สำหรับการสื่อสาร เป็นทักษะสำคัญสำหรับยุคปัจจุบัน

ทักษะนี้มีส่วนสำคัญอย่างมากในการทำงานร่วมกับคนอื่น และสามารถทำงานได้อย่างมีประสิทธิภาพเพิ่มมากขึ้น จึงขอแนะนำทักษะที่น่าศึกษา หรือฝึกฝนก่อนเริ่มทำงาน ดังนี้

1 การคิดอย่างมีวิจารณญาณ (Critical Thinking)

ความสามารถในการวิเคราะห์ข้อมูล และสถานการณ์อย่างมีเหตุผล เพื่อตัดสินใจ หรือแก้ปัญหาอย่างมีประสิทธิภาพ

2 การแก้ไขปัญหาและความคิดสร้างสรรค์ (Problem Solving & Creativity)

คิดหาวิธีแก้ไขปัญหาที่เป็นนวัตกรรม และสร้างสรรค์ความคิดใหม่ ๆ

3 ความรู้ความเข้าใจเกี่ยวกับสื่อ (Media Literacy)

ความสามารถในการวิเคราะห์ และสร้างสรรค์เนื้อหาสื่อในรูปแบบต่าง ๆ ทั้งเขียน ภาพ และวิดีโอ เพื่อการสื่อสารที่มีประสิทธิภาพ

4 ความรู้ความเข้าใจเกี่ยวกับข้อมูล (Data Literacy)

ความสามารถในการอ่าน วิเคราะห์ และใช้ข้อมูล เพื่อการตัดสินใจ หรือ การสื่อสารที่มีข้อมูลเชิงลึก

5 การรู้เท่ากันความปลอดภัยในโลกไซเบอร์ (Cybersecurity Awareness)

ความรู้ และความตระหนักรถกับภัยคุกคามในโลกดิจิทัล และการปกป้อง ข้อมูลส่วนบุคคล และข้อมูลขององค์กร

6 กักษะการสื่อสารข้ามวัฒนธรรม (Cross-cultural Communication Skills)

ความสามารถในการสื่อสารและทำงานร่วมกับผู้คนจากวัฒนธรรมต่าง ๆ

7 ความฉลาดทางอารมณ์ในโลกดิจิทัล (Emotional Intelligence in Digital Spaces)

ความสามารถในการตระหนักรู้ และจัดการกับอารมณ์ของตนเองและคนอื่น รวมถึงการสร้างความสัมพันธ์ที่ดีผ่านสื่อดิจิทัล

8 ความยืดหยุ่นและการปรับตัว (Adaptability and Flexibility)

ความสามารถในการปรับตัวต่อสถานการณ์ และการเปลี่ยนแปลงต่าง ๆ

9 ความคิดสร้างสรรค์ (Creativity)

ความสามารถในการคิดนออกรอบ สร้างสรรค์แนวคิดใหม่ๆ และหาทางออกที่ไม่เหมือนใคร

10 การทำงานร่วมกัน (Collaboration)

ความสามารถในการทำงานร่วมกับผู้อื่นอย่างมีประสิทธิภาพ แบ่งปันความคิดเห็น และแก้ไขปัญหาไปด้วยกัน

11 ภาวะผู้นำ (Leadership)

ความสามารถในการนำทีม สร้างแรงบันดาลใจ และผลักดันให้ทีมงานบรรลุเป้าหมายร่วมกัน

12 ความฉลาดทางวัฒนธรรม (Cultural Intelligence)

ความสามารถในการเข้าใจและทำงานร่วมกับผู้คนจากหลากหลายวัฒนธรรม

นอกจากทักษะเหล่านี้แล้ว อีกสิ่งสำคัญที่ขาดไม่ได้เลย คือ มารยาทในโลกดิจิทัล (Netiquette)



มารยาท ในโลกดิจิทัล (Netiquette)

มารยาทในโลกดิจิทัล (Netiquette)

เปรียบเสมือนกฎระเบียบ ที่ช่วยให้การสื่อสารออนไลน์เป็นไปอย่างราบรื่น ช่วยให้ผู้คนสามารถเชื่อมต่อ และสร้างความสัมพันธ์ที่ดีต่อกัน บนโลกออนไลน์ได้อย่างเหมาะสม โดยมีหลักการดังนี้

หลักการสำคัญของ มารยาทในโลกดิจิทัล (Netiquette)

1. เคารพผู้อื่น

ปฏิบัติต่อผู้อื่นด้วยความเคารพ เช่นเดียวกับที่เราต้องการได้รับการปฏิบัติไม่เหยียดหยามใคร

2. คิดก่อนพูด

พิจารณาเนื้อหาและผลกระทบของข้อความก่อนโพสต์หรือส่ง หลีกเลี่ยงความขัดแย้ง

3. รักษาความเป็นส่วนตัว

ไม่ควรเปิดเผยข้อมูลส่วนตัวของผู้อื่นโดยไม่ได้รับอนุญาต

4. รับผิดชอบต่อคำพูดและการกระทำ

ขอโทษหากสร้างความเสียหายให้ผู้อื่นและแก้ไขในสิ่งที่ทำผิดพลาด

5. รู้จักรอคอย

อดทนรอคอยการตอบกลับ หลีกเลี่ยงการส่งข้อความซ้ำ ๆ หรือรบกวนผู้อื่น

6. ใช้ภาษาที่เหมาะสม

เลือกใช้ภาษาที่สุภาพ เข้าใจง่าย หลีกเลี่ยงการใช้คำแสลง หรือคำหยาบคาย

7. ให้เกียรติเจ้าของลิขสิทธิ์

เคารพลิขสิทธิ์ของผู้อื่น ไม่แอบอ้างว่าเป็นผลงานของตน

8. แจ้งเตือนภัยออนไลน์

ช่วยเหลือผู้อื่นโดยแจ้งเตือนภัยออนไลน์

9. เป็นผู้ฟังก์ดี

เปิดใจรับฟังความคิดเห็นของผู้อื่น เคารพในความแตกต่าง

10. สนูกับโลกออนไลน์

ใช้เทคโนโลยีอย่างสร้างสรรค์ แบ่งปันสิ่งดี ๆ สร้างมิตรภาพ

สิ่งที่ควรปฏิบัติ ในการสื่อสารบนโลกดิจิทัล

1. ใช้ข้อความที่ชัดเจนและกระชับ เข้าใจได้ง่าย

หลีกเลี่ยงการใช้ภาษาที่คุณเครือ

2. หลีกเลี่ยงการใช้ภาษาที่ไม่เหมาะสม ไม่สุภาพ

คำที่มีลักษณะล่วงละเมิด หรือคำเสสลงที่อาจทำให้ผู้รับสารเข้าใจผิด

3. เคารพความเป็นส่วนตัวของผู้อื่น

ไม่ส่งต่อข้อมูลส่วนตัวหรือข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต

4. ตรวจสอบข้อความ และการสะกดคำก่อนส่งทุกครั้ง

เพื่อป้องกันข้อผิดพลาดและการเข้าใจผิด

5. ให้ความสำคัญกับการตอบกลับข้อความในเวลาที่เหมาะสม

หลีกเลี่ยงการทิ้งข้อความที่ต้องการการตอบกลับเป็นเวลานาน

6. Emoji ควรใช้ให้พอเหมาะ และเหมาะสม

จะช่วยแสดงความรู้สึกและทำให้ดูมีชีวิตชีวา แต่ ต้องใช้ให้พอเหมาะ และดูบริบทให้เหมาะสมสมด้วย

7. เคารพในความหลากหลาย

ของแต่ละวัฒนธรรมและบุคคล หลีกเลี่ยงการใช้คำ หรือข้อความที่อาจถูกตีความว่าเป็นการเลือกปฏิบัติหรือไม่เคารพ

สิ่งที่ควร และไม่ควรทำ ในโลกดิจิทัล



ถ้าเราอยากรีกษาภาระที่ในโลกดิจิทัลให้เริ่มจากการเรียนรู้สิ่งที่ควร และไม่ควรทำในโลกดิจิทัล ดังนี้

1. สิ่งที่ควรทำ



- ใส่ใจ และให้เกียรติผู้อื่นไม่ต่างจากโลกความจริง (Be Respectful)
- ตรวจสอบการส่งต่อข้อมูลให้ตรงกับกลุ่ม
- แบ่งปันสิ่งดี ๆ และสร้างสรรค์
- ปฏิบัติตามกฎของชุมชนออนไลน์

2. สิ่งที่ไม่ควรทำ



- แสดงความคิดเห็นด้วยถ้อยคำ犀利 แรง
- แสดงอารมณ์ขันที่หมิ่นเหม่ เสียดสี
- ส่งต่อข้อมูลที่เราไม่แน่ใจว่าเป็นความจริงหรือไม่
- ใช้โซเชียลมีเดียในการให้รายผู้อื่น



มารยาทในการ ประชุมออนไลน์

ปัจจุบันเนื่องจากเกิดการเปลี่ยนแปลงรูปแบบการทำงาน ทำให้การประชุม หรือการเรียนออนไลน์นั้น มีบทบาทในชีวิตของเรามากขึ้น สิ่งที่ไม่ควรลืม เลยคือ มารยาทในการประชุมออนไลน์ โดยมีวิธีปฏิบัติตัวง่าย ๆ ดังนี้

1. เข้าประชุมตรงต่อเวลา
2. เปิดกล้อง และเปิดฟังก์ชันเบลอพื้นหลัง เพราะบางครั้งฉกัด้านหลังของเราอาจไม่เรียบร้อย ซึ่งอาจจะส่งผลเสียต่อภาพลักษณ์ หรือรบกวนการประชุมได้
3. แต่งตัวให้เรียบร้อย แม้การประชุมออนไลน์จะเห็นเพียงร่างกาย ส่วนบนก็ควรจะแต่งตัวดีแต่ทรงผมให้เรียบร้อย เพื่อแสดงความพร้อม และความตั้งใจ
4. กดปุ่มยกมือก่อนพูด หรือเสนอความคิดเห็นทุกครั้ง
5. พยายามทำสภาพแวดล้อมให้เหมาะสมกับการประชุม เช่น หากคุณมีสัตว์เลี้ยงให้แยกออกไปอยู่อีกห้องหนึ่ง หรือไม่นั่งในที่ที่แสงมีดูนเงินไป





เสริมทักษะสำคัญประจำยุค
ไม่กระตุกการทำงานสัมฤทธิ์ผล
คิดสร้างสรรค์แก้ปัญหาไร้กังวล
ปรับตัวตนสร้างสัมพันธ์ผู้นำดี
และอิกสิ่งที่สำคัญอย่างไร้ขาด
มารยาทออนไลน์เป็นเกียรติศรี
คิดก่อนพูดรู้จักคolleyรับฟังดี
ใช้พาทีสุภาพสร้างมิตรเออย



ถ้าคุณเรียนผ่านด้านนี้
คุณจะมีส่วนช่วยหยุดวงจร
การกลั่นแกล้งบนโซเชียล
และไม่เสียงทำผิดกฎหมาย
ที่มีโทษสูงทั้งจำและปรับ

อ้างอิงข้อมูลจาก

<https://www.moj.go.th/view/56312>

4.4

CYBERBULLY

วัตถุประสงค์

- ผู้เรียนมีความรู้เกี่ยวกับ CYBERBULLY ได้
- ผู้เรียนสามารถเข้าใจถึงสิทธิดิจิทัลได้



การสื่อสาร เครื่องมือสำคัญ

ในการปกป้องสิทธิดิจิทัล



การสื่อสารทางดิจิทัล มีความสำคัญอย่างมากในยุคนี้ เพราะช่วยให้การสื่อสารเกิดขึ้นได้อย่างสะดวก รวดเร็ว และมีประสิทธิภาพ ไม่ว่าจะเป็นด้านธุรกิจ กระบวนการทำงานการศึกษา การใช้ชีวิตประจำวัน ช่วยให้ผู้คนสามารถเชื่อมต่อกันได้ไม่ว่าจะอยู่ที่ใดบนโลก ส่งผลให้เกิดการแลกเปลี่ยนข้อมูล ความคิดเห็น วัฒนธรรมที่หลากหลาย อีกทั้งยังเป็นเครื่องมือสำคัญในการสร้างความตระหนักรู้เกี่ยวกับสิทธิดิจิทัล และส่งเสริมให้ผู้คนเข้าใจ และปกป้องสิทธิของตนเอง

สิทธิดิจิทัล หรือ Digital Rights

REMEMBER

ถือเป็นสิทธิพื้นฐานที่ผู้คนควรมีเมื่อใช้งานเทคโนโลยีดิจิทัลและอินเทอร์เน็ต สิทธิเหล่านี้รวมถึงความเป็นส่วนตัว การเข้าถึงข้อมูลและบริการดิจิทัล การสื่อสาร การปกป้องจากการเฝ้าระวัง และการละเมิดข้อมูลส่วนบุคคล โดยไม่เหมาะสม จนไปถึงโอกาสในการพัฒนาทักษะดิจิทัล สิ่งที่ต้องคำนึงจากการใช้สิทธิดิจิทัลในมิติของการทำความเข้าใจเกี่ยวกับการไม่ละเมิดสิทธิของผู้อื่น ทั้งในด้านลิขสิทธิ์ของข้อมูล ประเด็นในด้านทรัพย์สินทางปัญญา การกลั่นแกล้งทางไซเบอร์ (Cyberbullying) และการคุกคามทางดิจิทัล (Digital Harassment)



"คนกำไม่เคยจดจำ แต่ผู้ถูกกระทำกลับไม่เคยลืม"

Cyberbully (การกลั่นแกล้งทางไซเบอร์)

จบอยู่แค่ช่วงเวลาวัยรุ่น จริงหรือ ?

ปัจจุบัน การกลั่นแกล้งทางไซเบอร์ เป็นปัญหาใหญ่ที่มีอยู่ทุกที่บนโลกออนไลน์ แม้กระทั่งสังคมการทำงาน การโドนการกลั่นแกล้งทางไซเบอร์ ก็ยังคงมีอยู่อย่างมากมาย ซึ่งมักจะมีเรื่องของการเมืองในที่ทำงานเข้ามา เกี่ยวข้อง ทำให้ทุกคนมีโอกาสที่จะเจอกับ การกลั่นแกล้งทางไซเบอร์ทั้ง นั้น ในไทยปัญหาการละเมิดสิทธิเด็กทัลที่เป็นเรื่องใหญ่องค์ดับตัน ๆ นั้น คือ การกลั่นแกล้งทางไซเบอร์

การกลั่นแกล้งทางไซเบอร์ (Cyberbully) ใคร ๆ เข้าก็ทำกัน... จริงหรือ ?

รูปแบบการข่มเหงรังแกทางโลกไซเบอร์

(Willard, 2007; Kowalski et al., 2014)

1. การประค่ารเม (Flaming)

คือ การโต้เถียงไปมาระหว่างบุคคล จนก่อเกิดความรุนแรง มีการใช้ถ้อยคำ ที่ก้าวร้าว และมีการดูถูกเหยียดหยาม มักเกิดขึ้นในพื้นที่สาธารณะ (เช่น ตามกระหุบอร์ดสนทนา) มากกว่าพื้นที่ส่วนตัว (เช่น อีเมล)

2. การก่อภัย (Harassment)

คือ การใช้ถ้อยคำหรือการกระทำใดๆ ที่สร้างความรำคาญใจและความทุกข์ใจต่อบุคคลหนึ่งโดยเจตนา โดยกระทำซ้ำ ๆ ส่วนใหญ่จะเกิดขึ้นในพื้นที่ส่วนตัว เช่น ช่องสนทนากลาง Facebook

3. การใส่ร้ายป้ายสี (Denigration)

คือการส่งต่อข้อมูลของบุคคลที่ไม่เป็นความจริง ผู้ส่งอาจนำข้อมูลไปเผยแพร่ในพื้นที่สาธารณะตามเว็บไซต์ต่าง ๆ รวมไปถึงพื้นที่ส่วนตัว

4. การปลอมตัวเป็นบุคคลอื่น (Impersonation)

การแอบอ้างเป็นบุคคลหนึ่ง และกระทำการสิ่งที่สร้างความเสื่อมเสียให้กับบุคคลนั้น เช่น ใช้ถ้อยคำหยาดกายด่าว่ากล่าวผู้อื่น เผยแพร่ข้อมูลที่ไม่เหมาะสมให้กับผู้อื่น ข่มเหงรังแกบุคคลอื่น เป็นต้น

การปลอมตัวเป็นบุคคลอื่น สามารถทำโดยการสร้างตัวตนเลียนแบบบุคคลนั้นขึ้นมาใหม่ หรือขโมยรหัสผ่านของบุคคลนั้นเพื่อใช้ตัวตนบนโลกออนไลน์ของบุคคลนั้นทำสิ่งที่ไม่เหมาะสม

5. การถ่ายคลิปวิดีโอและนำไปเผยแพร่ลงบนอินเทอร์เน็ต (Video Recording of Assaults)

คือ การนำคลิปวิดีโอไปเผยแพร่ตามที่ต่าง ๆ บนอินเทอร์เน็ต เพื่อสร้างความอับอายให้บุคคลนั้น

6. การส่งสั่งที่มีความล่อแหลมทางเพศ (Sexting)

คือ การส่งข้อความ รูปเปลือย หรือรูปเกี้ยงเปลือยที่มีความล่อแหลมทางเพศให้กับผู้อื่น

บางครั้ง ก็เพลオเพิ่มความรุนแรงของการกลั่นแกล้ง ด้วยการพูดถึงประเด็นของคนที่ถูกบูลลี่ เพราะเห็นว่าใคร ๆ ก็ทำกัน หักห้ามห้ามไม่ได้ ออนไลน์แบบทุกครั้งเกิดจากความตั้งใจ แต่บางคนก็ใช้ข้ออ้างว่า “อีกฝ่ายอ่อนแอะเอง” มาเป็นข้ออ้างลดความรู้สึกผิดในจิตใจ

อ่อนแอกับแพ้ไป

เป็นวิธีที่บ่งชี้ว่าปัจจุบันหลายคนมองว่าทุกอย่างคือ การแข่งขัน ต้องการเอาชนะ ต้องการเป็นที่สนใจ ใครที่ไม่ไหวก็ยอมแพ้ไปซะ อาจจะตีความได้ว่าบางครั้งสาเหตุหลักของการกลั่นแกล้งทางไซเบอร์นี้ คือการที่ไม่ต้องการให้ใครโดดเด่นกว่าตัวเอง

ทำไมบางคนไม่ตระหนักรู้ ความรุนแรงของการกลั่นแกล้ง ทั้งที่มันทำร้าย และคร่าชีวิตคนได้ ?

ส่วนหนึ่งน่าจะเป็น เพราะความรู้สึกไม่ชอบใจคนที่ตัวเองแกล้ง และอาจ เพราะรู้สึกว่าหลายอย่างบนโลกออนไลน์โผล่ขึ้นมา เป็นประเด็นดราม่า แล้วซักพักก็ผ่านไป พอดีซึ่งหนึ่งทุกคนก็พากันลืมหมด แต่เราอาจจะลืมไปว่า... รอยแผลเป็นบางครั้งก็ยากที่จะลบเลือน เช่นเดียวกับคนที่โดนกีดกันที่จะลืม อาจจะพูดติดตลกว่า เดี๋ยวนี้รอยแผลเป็นเราก็ใช้เทคโนโลยีลบออกได้ แต่ทั้งนี้มันก็ไม่ได้ง่าย ลองคิดเล่น ๆ ดูว่า ทุกคนต่างมีแผลใจในวัยเด็กกันทั้งนั้น บางคนใช้เวลารักษาแผลใจทั้งชีวิตยังรักษาไม่หาย ยังจำมันได้ขึ้นใจเจ็บปวดกับมัน หวานกับมัน ทำให้เมื่อไรขอ疤แผลใจเหล่านี้ และการบูลลี่ คือ การที่สร้างแผลใจที่รักษาได้ยากนี้ให้กับคนอื่น

สิ่งที่กำให้เกิด การกลั่นแกล้งทางไซเบอร์ ได้จำนวนมาก คือ

ความยกในการติดตาม และระบุตัวการ มันเป็นความสะใจอย่างหนึ่งที่เห็นผู้ถูกกระทำกระวนกระวายกับสิ่งที่เกิดขึ้น แต่หาต้นต่อไม่เจอเนื่องจากคนทำสามารถซ่อนตัวตนบนโลกออนไลน์ได้และเมื่อมันเป็นกระแสก็จับมือใคร

ดูไม่ได้ ซึ่งมันง่ายมากที่จะโพสต์พูดถึงคนอื่น ยิ่งเป็นคนที่เราไม่ชอบหน้า เรายังรู้สึกว่าไม่ต้องสนใจน้ำใจ ยิ่งการแซะการด่าันนี้มีจังหวะที่สนุก สะใจ หน่อย ๆ ทำให้วางแผนมีความสนุกสนาน มันก็รู้สึกว่าเป็นเรื่องที่ทำได้ และอาจเลยถูกใจไปจนถึงการใส่สีตีไช่ ใส่ความเป็นคนไม่ดีให้ ซักจุ่งให้ทุก คนเกลียดคน ๆ นั้น จนนำไปสู่การลงมือกลั่นแกล้งในที่สุด

กี่นากรังสรรค์ การบูรลี่ กันมีอยู่ แบบทุกสังคม ไม่เว้นแม้กระทั่งในสังคม ที่ทำงาน

- แพร่กระจายข่าวลือผิดเกี่ยวกับตัวเราในที่ทำงาน
- ดิสเครดิตเพื่อไม่ให้ได้รับความไว้ใจ
- โพสต์ความเห็นเชิงลบเกี่ยวกับเรา จนเราเดือดร้อน
- ไม่ถูกยอมรับในที่ทำงาน ทุกคนตั้งแต่ แลและทึ่งให้โดยเดียว
- หนักหน่อยหลายคนอาจจะเจอกับความเห็นต์เชิงล้อเลียน หรือ Sexual Harassment จากคนในที่ทำงาน





การจัดการกับ Cyberbully

ต้องเริ่มจาก ความเข้าใจ ว่า มันไม่ใช่เพียงการกลั่นแกล้งกันเล็กน้อยและไม่มีใครอยากรให้เกิดกับตัวเอง เพราะร่องรอยดิจิทัลนี้สามารถถ่ายทอดไปมันไม่ได้หายไป มันลบไม่ได้ วันเดือนดีก็จะย้อนกลับมา ยิ่งมันกลับมา ในช่วงที่เหยียบกว่าทุกอย่างมันเดี๋ยวแล้ว ก็จะยิ่งเจ็บปวดมากขึ้น

มีหลากหลายวิธีการ โดยอาศัยการร่วมมือระหว่างหน่วยงาน องค์กร ไม่单单ทางผลกำไร โรงเรียน และชุมชนออนไลน์ เพื่อสร้างสภาพแวดล้อมที่ปลอดภัยและรับมือกับปัญหาการกลั่นแกล้งทางอินเทอร์เน็ต

ในต่างประเทศนั้น หลายประเทศได้พัฒนากฎหมาย และนโยบาย เพื่อต่อสู้กับ Cyberbully โดยเฉพาะ รวมถึงการกำหนดความผิดทางอาญาสำหรับการกลั่นแกล้งทางอินเทอร์เน็ต และการสร้างกรอบในการทำงานสำหรับโรงเรียน และองค์กรในการรายงานและจัดการกับเหตุการณ์ รวมไปถึง การรณรงค์วิธีการป้องกัน

รวมถึงการจัดการกับปัญหานี้ เป็นกลยุทธ์หลักที่สถานศึกษา และองค์กร ต่าง ๆ มักจัดการรณรงค์เพื่อเพิ่มความตระหนักรและสร้างทักษะการจัดการ

กับการกลั่นแกล้งในโลกไซเบอร์ พร้อมกันนี้ หลายแพลตฟอร์มออนไลน์และโซเชียลมีเดียได้พัฒนาเครื่องมือ ให้ผู้ใช้สามารถรายงานเนื้อหาที่เป็นการกลั่นแกล้งได้ง่ายขึ้น ทำให้ผู้ดูแลระบบสามารถดำเนินการลบเนื้อหาหรือบัญชีที่มีพฤติกรรมการกลั่นแกล้งได้อย่างรวดเร็ว แต่สิ่งสำคัญ คือ การพัฒนาทักษะดิจิทัลและการมโนให้กับเด็กและวัยรุ่น เพื่อช่วยให้พวกเขารู้สามารถจัดการกับสภาพแวดล้อมออนไลน์ได้อย่างปลอดภัยและเหมาะสม

ตัวอย่างการจัดการปัญหา CYBERBULLY ในต่างประเทศ



สหรัฐอเมริกา

- มีการต่อต้าน Cyberbullying ทั้งในระดับรัฐและระดับชาติ
- หลายรัฐมีกฎหมายที่เฉพาะเจาะจงเกี่ยวกับ Cyberbullying
- กำหนดให้โรงเรียนมีนโยบายและโปรแกรมป้องกันการกลั่นแกล้งทางอิเล็กทรอนิกส์ องค์กร เช่น StopBullying.gov ให้ข้อมูลและทรัพยากรเพื่อช่วยเหลือหั้งผู้ที่ถูกกลั่นแกล้งและผู้ที่ต้องการป้องกันการกลั่นแกล้ง

อสเตรเลีย

- มี eSafety Commissioner ซึ่งเป็นหน่วยงานของรัฐบาลที่รับผิดชอบในการป้องกันและต่อต้านการกลั่นแกล้งทางอินเทอร์เน็ต หน่วยงานนี้ให้บริการแนะนำ การสนับสนุน และทรัพยากรสำหรับผู้ที่ได้รับผลกระทบจาก Cyberbullying และมีอำนาจในการดำเนินการกับเนื้อหาที่เป็นการกลั่นแกล้งบนแพลตฟอร์มออนไลน์

สหราชอาณาจักร

- มีการริเริ่มโครงการต่าง ๆ เช่น Anti-Bullying Alliance
- โครงการที่สนับสนุนโดยรัฐบาล เช่น UK Safer Internet Centre ที่มีเป้าหมายเพื่อเพิ่มความตระหนัก การศึกษา และการป้องกัน Cyberbullying
- กฎหมายอาญาของสหราชอาณาจักรก็สามารถใช้ดำเนินคดีกับการกระทำของ Cyberbullying ในบางกรณีได้

แคนาดา

- มีการใช้กฎหมายและนโยบายเพื่อต่อสู้กับ Cyberbullying
- ปรับปรุงกฎหมายอาญา เพื่อรวมถึงการคุกคามทางอิเล็กทรอนิกส์
- มีการจัดตั้งศูนย์ทรัพยากรออนไลน์ เช่น PrevNet ซึ่งให้ข้อมูล และทรัพยากรสำหรับผู้ปกครอง ครู และเยาวชนเพื่อช่วยเหลือในการต่อสู้กับการกลั่นแกล้ง

วิธีการรับมือกับการกลั่นแกล้งทางไซเบอร์

Stop



คือหยุด ไม่ต้องไปตอบโต้ เสียเวลาไปใส่ใจกับคนนิสัยไม่ดีที่กลั่นแกล้งเรา หรือคุกคามเราทางออนไลน์ รวมทั้งบล็อกคนพากันไปเลยยิ่งดี

Tell



คือบอกหรือปรึกษาผู้ใหญ่ที่เราไว้ใจหรือพูดคุยกับ ไม่ว่าจะพ่อแม่ ผู้ปกครอง หรือคุณครู

Del ย่อมาจาก Delete



คือบอกคนที่แกล้งให้ลบ ถ้าเขามีเลบก็แจ้งคุณครู หรือแจ้งให้ผู้ดูแลระบบ ลบโพสต์นั้นออก ที่สำคัญคือลบเรื่องที่ไม่เป็นจริงหรือทำร้ายจิตใจออกไป จากความคิดเราด้วย

Strong



คือยืนรับสิ่งที่เกิดอย่างเข้มแข็ง และใช้เป็นแรงผลักดันให้ชีวิตเราดีขึ้น

สำหรับผู้ใหญ่ ผู้ปกครอง ครู อาจารย์ รวมทั้งคนแวดล้อม "Digital Resilience" หรือ ภูมิคุ้มกันในโลกดิจิทัล

ถือเป็นอีกแนวทางที่สำคัญ ที่จะทำให้เด็กสามารถรับมือกับภัยไซเบอร์ต่าง ๆ รวมทั้งเรื่อง Cyberbullying ด้วย การสร้างภูมิคุ้มกันเพื่อการใช้ออนไลน์ ได้อย่างปลอดภัยและมีประสิทธิภาพ ต้องอาศัยองค์ประกอบ 3 อย่าง ร่วมกัน ได้แก่

1 ก้าวทางดิจิทัล (The Youth Digital Skill)

ความสามารถในการใช้เทคโนโลยีและการสื่อสารเพื่อผลิตผลงาน รวมถึง การแสดงสื่อต่าง ๆ อย่างมีวิจารณญาณ

2 การมีภูมิคุ้มกันทางใจ (Resilience)

คือ ความสามารถในการรับมือและยืนหยัดเผชิญหน้ากับปัญหา จนสามารถ พึ่นพูจิจิใจของตัวเองได้หลังจากผ่านเหตุการณ์เหล่านั้นไป

3 ปัจจัยปกป้องในการใช้อินเทอร์เน็ต (Digital Protective Factor)

คือ สิ่งที่ช่วยทำให้เกิดการปรับตัวเพื่อสร้างเกราะป้องกันผลกระทบทางลบ

หลักปฏิบัติ ที่ช่วยให้เราสามารถ จัดการกับความเสี่ยงที่อาจจะต้อง^{พบรอได้ในอนาคต}

มีด้วยกัน 4 ข้อ ดังนี้

1. รู้ตัวว่าเมื่อใดที่ตนเองตกอยู่ในความเสี่ยง
2. รู้ว่าต้องทำอย่างไรเพื่อขอความช่วยเหลือหากเจอภัยออนไลน์
3. เรียนรู้จากประสบการณ์ของตนเอง
4. รู้จักวิธีการ gob กู้สถานการณ์เมื่อเกิดปัญหา

ทั้งนี้ คนรอบตัวต้องเข้าใจถึงความร้ายแรงของเหตุการณ์ สิ่งที่สำคัญที่สุด ไม่ใช่การดูด่า ไม่ว่าจะด้วยความโกรธหรือความเป็นห่วง แต่เป็นการรักษา จิตใจของคนที่โดนกระทาให้สามารถรับมือปัญหาให้ผ่านพ้นไปได้

การไม่เป็นส่วนหนึ่งของการบูลลี่อาศัยแค่ตัวเราเท่านั้น แค่คิดว่า เรื่องนี้ แพร่ออกไปแล้วจะทำร้ายใครใหม่ หลังจากนั้นมีคนที่นั่งอยู่เหมือนกัน คนที่อาจจะทั้งถูกหรือผิดก็ได้ ทุกอย่างอาจเป็นเรื่องเข้าใจผิดก็ได้ แค่คุณ หยุดมือ และฉุกคิดก็ถือว่าเริ่มต้นที่ดีแล้ว





ปัญหาใหญ่และเมิดลิทธิจิทัล
 การแกล้งกันข่มเหงทางไซเบอร์
 ทั้งรูปแบบติดตามยามเมื่อเพลオ
 พูดเพ้อเจ้อใส่ร้ายปลอมตัวตน
 ทั้งค่าว่าบาร์โต้เกียงแฉแพร์ก้าพหลุด
 ไม่สิ้นสุดความรุนแรงขยายผล
 ผู้กระทำการหยุดยั้งคิดกลับตน
 ถ้าเป็นคนโคนบ้างจะเป็นไง ?!

4.1 Digital Footprint Management

ร่องรอย
การสื่อสาร

การสื่อสารดิจิทัล

ร่องรอยดิจิทัล

ประเภทของ
Digital Footprint

เครื่องมือในการจัดการ Digital Footprint

ตั้งค่าความเป็นส่วนตัว
อย่างเข้มงวด
บนโซเชียลมีเดีย

ลบประวัติการค้นหาและ
คุกเก็ต (Cookie) เป็นประจำ

ใช้ VPN ในกรณี
ต้องใช้ Wi-Fi สาธารณะ

ร่องรอยดิจิทัล
เชิงบวก และเชิงลบ

ร่องรอยดิจิทัลเชิงบวก

ร่องรอยดิจิทัลเชิงลบ

12 เหตุผลที่
Digital Footprint
คือสิ่งสำคัญต่อ HR

เปิดสถิติ Digital Footprint
คือหนึ่งในเหตุผล
การรับผนักงานใหม่

3 อันดับ
Digital Footprint
ร้ายแรงที่จะไม่รับเข้าทำงาน

3 อันดับ
Digital Footprint
เป็นประโยชน์ต่อการรับเข้าทำงาน

กักษะพื้นฐาน
สื่อสารอย่างเข้าใจ

สิ่งที่ทำให้
การสื่อสารดิจิทัล
ประสบความสำเร็จ

การสื่อสารระหว่างบุคคล

การสื่อสารระหว่างกลุ่มคน

การเลือกใช้เทคโนโลยี เพื่อการสื่อสารอย่างสร้างสรรค์

การรับมือดับ
ประดิษฐ์สื่อสารทางลบ

ระดับบุคคล

ระดับองค์กร

4.2 Interaction & Collaboration

ปัจจัยที่ทำให้การสื่อสาร
ประสบความสำเร็จ
หรือล้มเหลว

เครื่องมือสื่อสารดี
มีชัยไปกว่าครึ่ง

วิเคราะห์สุดเฉียบ
เพียงพร้อมด้วยแนวทาง

การสื่อสาร
ระหว่างกลุ่มคน
แบบเป็นสาธารณะ

เนื้อหาชัดเจน
สื่อสารฉับไว

สื่อสารอย่างเข้าใจ
ดีต่อใจคุณผู้ฟัง

เข้าใจความต่าง
หนทางของผู้อยู่เบื้อง

ภาพจำดี มีมารยาท

รับสารอย่างดี
เพิ่มศักยภาพความเข้าใจ

4.3 Future Skill

Future Skill
สำหรับการสื่อสาร
ทักษะสำคัญในยุคปัจจุบัน

สิ่งที่ควร และไม่ควรทำ
ในโลกดิจิทัล

สิ่งที่ควรทำ

ให้เจ้า
และให้เรียดผู้อื่น

ตรวจสอบ
การส่งต่อข้อมูล

แบ่งบันลิ้งดี ๆ

ปฏิบัติ
ตามกฎของชุมชน

สิ่งที่ไม่ควรทำ

ใช้อ้อยคำรุนแรง

หมิ่นเหม่ เสียดสี

ส่งต่อข้อมูลเท็จ

ให้ร้ายผู้อื่น

มารยาท
ในโลกดิจิทัล
(Netiquette)

หลักการสำคัญ
ของ มารยาท
ในโลกดิจิทัล

สิ่งควรปฏิบัติ
ในการสื่อสาร
บนโลกดิจิทัล

มารยาทในการ
ประชุมออนไลน์

เข้าประชุมตรงต่อเวลา

เปิดกล้อง และเปิด
ฟังก์ชันเบล็อกพื้นหลัง

แต่งตัวให้เรียบร้อย

กดปุ่มยกมือก่อนพูด

ทำสภาพแวดล้อมให้
เหมาะสมกับการประชุม

4.4 Cyberbully

การสื่อสารเครื่องมือสำคัญ
ในการปักป้อง สิติกดิจิทัล

สิทธิดิจิทัล หรือ
Digital Rights

การกลั่นแกล้งทางไซเบอร์
ใคร ๆ เขาก็ทำกัน...
จริงหรือ ?

ทำไมบางคนไม่ตระหนักรถึง
ความรุนแรงการกลั่นแกล้ง
ทางไซเบอร์ ?

สิ่งที่ทำให้เกิด
การกลั่นแกล้งทางไซเบอร์

การบูลลี่มีแบบทุกสัมคม
ไม่ว่าแม้กระทั่งในสังคมที่ทำงาน

"คนทำไม่เคยวอดจำว่า
แต่ผู้ถูกกระทำกลับไม่เคยลืม"

วิธีการรับมือดับ
การกลั่นแกล้งทางไซเบอร์

สำหรับผู้ใหญ่ ผู้ปกครอง
ครู อาจารย์
รวมทั้งคนแวดล้อม

หลักปฏิบัติ ที่ช่วยให้เรา
สามารถจัดการกับความเสี่ยง

การจัดการ
กับ Cyberbully

ตัวอย่างการจัดการ
Cyberbully
ในต่างประเทศ

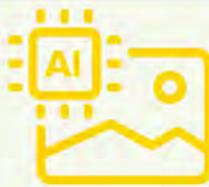
สหรัฐอเมริกา

ออสเตรเลีย

สาธารณรัฐอินเดีย

แคนาดา

05



การรู้เท่ากันดิจิทัล

— Digital Literacy —

ແນະນຳສໍາຮັບຜູ້ສວນ



• ວັດຖປະສົງຄ່າ

ຜູ້ເຮັດວຽກມີຄວາມຮູ້ເກີດຈິນ ຈາກການນຳເສັອເນື້ອທາທີ່ໄມ່ນໍາເຊື່ອຄື່ອງ
ແລະອົບາຍື່ງຄວາມແຕກຕ່າງ ຄວາມຫລາກຫລາຍຂອງແໜ່ງຂໍ້ມູນ ແລະຄວາມນໍາເຊື່ອຄື່ອງ
ຂອງຂໍ້ມູນທີ່ຈຸດວຽກຈາກສໍອດິຈິທັກໄດ້

• ຂອບເຂດຕະຫຼາດນີ້

5.1 Media & Information

- ແລ້ວຂໍ້ມູນດິຈິທັກ ວັນທີສອນ
...../...../.....
- ດຽວມາຕິຂອງສື່ອ ວັນທີສອນ
...../...../.....
- ແນວດການໃນການຮັບຮມສື່ອຢ່າງຮູ້ເທົ່າຫັນ ວັນທີສອນ
...../...../.....
- ການປະເມີນຄຸນກາພ / ຄວາມນໍາເຊື່ອຄື່ອງຂອງຂໍ້ມູນ
ຈາກສໍອດິຈິທັກ ວັນທີສອນ
...../...../.....
- ຮູ້ເທົ່າຫັນ Fake News ປັບປຸງກັນຄວາມເສີຍງານຈາກສໍອດິຈິທັກ ວັນທີສອນ
...../...../.....
- ແນວດການແລກປ່ຽນປະສບກາຮນໃນການຈັດກາ
ຂໍ້ມູນຈາກສໍອດິຈິທັກ ວັນທີສອນ
...../...../.....
- ການແບ່ງປິນເນື້ອທາທີ່ໄມ່ເໜັກສົນ ວັນທີສອນ
...../...../.....

5.2 Digital Content Creation

- สื่อดิจิทัล วันที่สอน
/ / / ...
- แนวทางการสร้างเนื้อหาดิจิทัลให้ดีและโดนใจ วันที่สอน
/ / / ...
- แนวทางสร้างเนื้อหาดิจิทัลให้ดึงดูดและสร้างการจดจำ วันที่สอน
/ / / ...
- หลักการสร้างเนื้อหาให้ถูกกฎหมายและมีจริยธรรม วันที่สอน
/ / / ...
- พฤติกรรมการสร้างเนื้อหาและสื่อที่ละเอียดกฎหมาย วันที่สอน
/ / / ...
- ลิขสิทธิ์กับ CREATIVE COMMONS วันที่สอน
/ / / ...
- การอ้างอิงแหล่งข้อมูล (Citation) ในงานวิจัย วันที่สอน
/ / / ...

5.3 Data & AI Governance

- ทำความเข้าใจ AI วันที่สอน
/ / / ...
 - ประเภทของ AI วันที่สอน
/ / / ...
 - ความแตกต่างระหว่าง AI, Machine Learning และ Deep Learning วันที่สอน
/ / / ...
 - โอกาสจากการใช้ประโยชน์จาก AI วันที่สอน
/ / / ...
 - ความท้าทายในการใช้ประโยชน์จาก AI วันที่สอน
/ / / ...
 - การใช้ AI ในชีวิตประจำวัน วันที่สอน
/ / / ...
 - การใช้ประโยชน์จาก AI อย่างมีธรรมาภิบาล วันที่สอน
/ / / ...
 - ความเสี่ยงจากการใช้เทคโนโลยี AI วันที่สอน
/ / / ...
 - Do / Don't ในการใช้ AI วันที่สอน
/ / / ...
 - อนาคตของ AI วันที่สอน
/ / / ...
- เวลาในการเรียน

รู้ศัพท์ ไม่สับสน



1



FAKE NEWS

คือ ข่าวปลอมหรือข่าวสารที่ไม่มีความจริง

2



INFORMATION DISORDER

เป็นการรวมคำสองคำเข้าด้วยกันจาก INFORMATION (ข่าวสาร) และ EPIDEMIC (การระบาด) โดยข้อมูลในลักษณะนี้ถือเป็น ความผิดปกติของข้อมูลข่าวสาร (INFORMATION DISORDER)

4

3



MISINFORMATION

ข้อมูลที่ผิด คือ ข้อมูลที่ไม่ถูกต้อง หรือข้อมูลเท็จ โดยผู้ส่งอาจไม่รู้หรือไม่ได้เจตนาต่อการเผยแพร่ข้อมูลที่ผิด



DISINFORMATION

หรือข้อมูลที่ถูกบิดเบือน

คือ ข้อมูลที่ผู้ส่งตั้งใจสื่อสารอกรมา อาจเป็นข้อมูลจริงบางส่วนที่เรียกว่า “ความจริงครึ่งเดียว” (HALF-TRUTH)

รู้ศัพท์ ไม่สับสน



5



MALINFORMATION

ข้อมูลที่แฝงเจตนาร้าย คือ ข้อมูลที่นำมาจากข้อเท็จจริง เพื่อคำนวณทำร้ายเป้าหมาย โดยการนำข้อมูลความลับที่ละเอียดความเป็นลับตัวของผู้อื่นออกมายังเปิดเผยในที่สาธารณะ เพื่อหวังที่จะโฉนดให้เกิดความเสียหายอันตราย

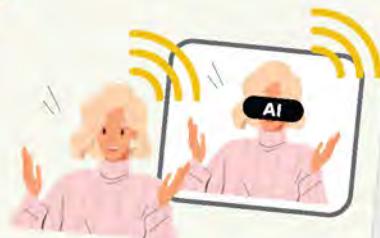
6



DEEPCODE

คือ GENERATIVE AI รูปแบบหนึ่ง ที่สามารถสร้างสื่อสังเคราะห์ทั้งภาพนิ่ง เสียง ภาพเคลื่อนไหวพร้อมเสียง ที่เหมือนเป็นคนมาพูดหรือคุยจริง ๆ จนแบบแยกไม่ออก ด้วยระบบการเรียนรู้ หรือ DEEP LEARNING

8



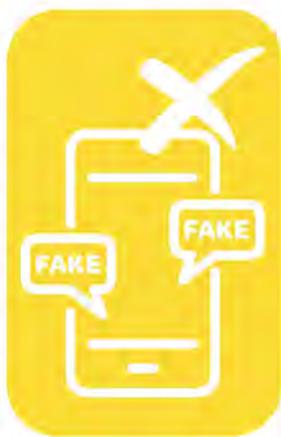
VOICE CLONING

คือ การใช้ AI ปลอมเสียง โดยจะเป็นการใช้ AI เลียนแบบเสียงของบุคคล ให้มีความคล้ายคลึงกับบุคคลจริง



FAKE BUSINESS

คือ การใช้ GENERATIVE AI ในการสร้างบทความหรือสคริปต์วิดีโอ เพื่อให้ดูเป็นมืออาชีพ



ถ้าคุณเรียนผ่านด้านนี้
คุณจะมีภูมิคุ้มกัน
ด้านข่าวลวงข้อมูลเท็จ
และไม่ตกเป็นเหยื่อโจรออนไลน์

5.1

MEDIA & INFORMATION

วัตถุประสงค์

- ผู้เรียนสามารถอธิบายถึงความแตกต่าง และหลากหลายของแหล่งข้อมูล และการได้มาซึ่งข้อมูลที่ตรงกับความต้องการบนโลกดิจิทัลได้
- ผู้เรียนสามารถเข้าใจถึงวิธีการค้นหาข้อมูล รวบรวม และจัดการข้อมูล ที่ต้องการจากสื่อดิจิทัลได้
- ผู้เรียนสามารถเข้าใจถึงการประเมินคุณภาพ และความน่าเชื่อถือของ ข้อมูล และเลือกใช้ข้อมูลที่สอดคล้องกับความต้องการได้
- ผู้เรียนสามารถตระหนักรถึงผลกระทบที่เกิดขึ้นจากการนำเสนอ หรือ แบ่งปันเนื้อหาที่ไม่น่าเชื่อถืออาจก่อให้เกิดความเข้าใจผิด หรือหลงเชื่อได้

รู้เท่าทันดิจิทัล

ทักษะจำเป็นเพื่อชีวิตออนไลน์



ในปัจจุบัน ที่เนื้อหาข้อมูลข่าวสารเพิ่มขึ้น และไฟฟ้านอย่างรวดเร็ว อันเกิดจากสื่อที่มีมากขึ้น รวมถึง สื่อออนไลน์ที่ง่ายต่อการบริโภค และ การส่งต่อ ดังนั้น “ความรู้เท่าทันดิจิทัล” จึงเป็นทักษะที่จำเป็นในการ เข้าถึงแหล่งข้อมูลดิจิทัลให้ตรงกับความต้องการ เข้าใจ ประเมินค่า และ ใช้สื่อเหล่านี้อย่างมีประสิทธิภาพและปลอดภัย





ก่อนอื่นเรามารู้จักกับ แหล่งข้อมูลดิจิทัล กันก่อน

REMEMBER

แหล่งข้อมูลดิจิทัล คือ ข้อมูลหรือสารสนเทศที่บันทึกในรูปแบบดิจิทัล สามารถจัดเก็บ ประมวลผล และเผยแพร่ผ่านสื่ออิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ อุปกรณ์พกพา เครือข่ายอินเทอร์เน็ต เป็นต้น

รูปแบบของแหล่งข้อมูลดิจิทัล

มีรูปแบบที่หลากหลาย ขึ้นอยู่กับประเภทของข้อมูล หรือสารสนเทศที่บันทึกไว้ เช่น

- ข้อความ

เช่น หนังสือ บทความ เอกสารทางวิชาการ กฎหมาย จดหมาย เป็นต้น

- ภาพ

เช่น ภาพถ่าย ภาพวาด กราฟิก แผนภูมิ เป็นต้น

- เสียง

เช่น เพลง เสียงพูด เสียงประกอบ เป็นต้น

- วิดีโอ

เช่น ภาพยนตร์ รายการโทรทัศน์ คลิปวิดีโอ เป็นต้น

- ข้อมูลเชิงตัวเลข

เช่น สถิติ ตัวเลข ข้อมูลทางการเงิน เป็นต้น

เกณฑ์การแบ่งประเภทของแหล่งข้อมูลดิจิทัล

แหล่งข้อมูลดิจิทัลสามารถแบ่งประเภทได้หลายประเภท โดยใช้เกณฑ์ที่แตกต่างกัน เช่น

1 แบ่งตามแหล่งที่เผยแพร่ข้อมูล

แบ่งได้ 2 ประเภท คือ

- การสร้างหรือผลิตข้อมูลโดยเจ้าของแหล่งข้อมูล หรือเจ้าของเว็บไซต์ เช่น ข้อมูลจากเว็บไซต์โรงพยาบาล หน่วยงานรัฐ หรือเอกชนต่าง ๆ ที่มีการเผยแพร่ข้อมูล เป็นต้น
- การสร้างหรือผลิตข้อมูลโดยชุมชนผู้ใช้งาน เช่น เพชบุ๊ก พันทิป หรือโซเชียลมีเดียต่าง ๆ เป็นต้น



2 แบ่งตามสังกัดการเข้าถึงข้อมูล

แบ่งได้ 2 ประเภท คือ

- แหล่งข้อมูลที่เข้าถึงได้โดยเสรี เช่น เว็บไซต์ที่เผยแพร่ข้อมูลข่าวสารทั่วไป หรือโซเชียลมีเดียทั่วไป เป็นต้น



- แหล่งข้อมูลที่จำกัดการเข้าถึง

ซึ่งสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตที่มีส่วนเกี่ยวข้องเท่านั้น เช่น ระบบทะเบียนราษฎร ฐานข้อมูลของภาครัฐ ระบบข้อมูลของบริษัทเอกชน เป็นต้น



3 แบ่งตามประเภทของข้อมูล

สามารถแบ่งได้หลายประเภท เช่น

- แหล่งข้อมูลเพื่อการศึกษาเรียนรู้
- แหล่งข้อมูลเพื่อความบันเทิง
- แหล่งข้อมูลด้านสุขภาพ
- แหล่งข้อมูลด้านธุรกรรมและการเงิน
- แหล่งข้อมูลด้านเศรษฐศาสตร์และธุรกิจ



4 แบ่งตามรูปแบบการนำเสนอข้อมูล

สามารถแบ่งได้ 2 ประเภท ได้แก่

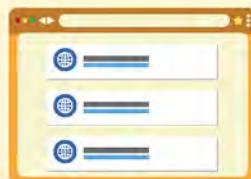
- แหล่งข้อมูลแบบคงที่ (Static)

คือ แหล่งข้อมูลที่มีรูปแบบการนำเสนอที่ตายตัว
ไม่สามารถเปลี่ยนแปลงได้ เช่น เอกสาร PDF
รูปภาพ วิดีโอ เป็นต้น



- แหล่งข้อมูลแบบไดนามิก (Dynamic)

คือ แหล่งข้อมูลที่มีรูปแบบการนำเสนอที่
สามารถเปลี่ยนแปลงได้ เช่น เว็บไซต์
แอปพลิเคชัน เป็นต้น



5 แบ่งตามลักษณะการใช้งานได้

สามารถแบ่งได้ 2 ประเภท ได้แก่

- แหล่งข้อมูลสาธารณะ (Public)

คือ แหล่งข้อมูลที่สามารถเข้าถึงได้โดยไม่จำกัด เช่น เว็บไซต์ของรัฐบาล เว็บไซต์ขององค์กรต่าง ๆ เว็บไซต์ของสถาบันการศึกษา เป็นต้น



- แหล่งข้อมูลส่วนตัว (Private)

คือ แหล่งข้อมูลที่สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์ เท่านั้น เช่น เว็บไซต์ขององค์กรที่มีระบบบรักษาความปลอดภัย เว็บไซต์ของบุคคลที่มีรหัสผ่าน เป็นต้น



6 แบ่งตามลักษณะการเผยแพร่

สามารถแบ่งได้ 2 ประเภท ได้แก่

- แหล่งข้อมูลแบบออนไลน์ (Online)

คือ แหล่งข้อมูลที่สามารถเข้าถึงได้ผ่านเครือข่ายอินเทอร์เน็ต เช่น เว็บไซต์ แอปพลิเคชัน เป็นต้น



- แหล่งข้อมูลแบบออฟไลน์ (Offline)

คือ แหล่งข้อมูลที่สามารถเข้าถึงได้โดยไม่ต้องใช้เครือข่ายอินเทอร์เน็ต เช่น หนังสือ เอกสาร PDF รูปภาพ วิดีโอ เป็นต้น



ประโยชน์ของแหล่งข้อมูลดิจิทัล

1. เข้าถึงข้อมูลได้ง่ายและรวดเร็ว



2. สามารถจัดเก็บข้อมูลได้เป็นจำนวนมาก



3. สามารถแบ่งปันข้อมูลได้อย่างรวดเร็ว



4. สามารถแก้ไขข้อมูลได้สะดวก



5. สามารถใช้งานร่วมกับอุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ได้



6. ช่วยให้การเรียนรู้ ทำงาน หรือการสื่อสารมีประสิทธิภาพมากขึ้น

ตัวอย่างแหล่งข้อมูลดิจิทัล

- เว็บไซต์

เช่น Google Search, Wikipedia, YouTube, Facebook, X (Twitter) เป็นต้น

- ห้องสมุดดิจิทัล

เช่น Digital Library of Thailand, Thai Digital Library เป็นต้น

- ฐานข้อมูล

เช่น ฐานข้อมูลวิชาการ
ฐานข้อมูลกฎหมาย
ฐานข้อมูลธุรกิจ เป็นต้น

- ซอฟต์แวร์

เช่น ซอฟต์แวร์ประมวลผลคำ (Word Processing)
ซอฟต์แวร์กราฟิก (Graphic)
ซอฟต์แวร์นำเสนอ (Presentation)

การเลือกใช้งานแหล่งข้อมูลดิจิทัล

ควรพิจารณา ดังนี้

1) พิจารณาวัตถุประสงค์การใช้งาน



ต้องการข้อมูลหรือสารสนเทศประเภทใด

2) พิจารณาความน่าเชื่อถือของแหล่งข้อมูล



เป็นแหล่งข้อมูลที่น่าเชื่อถือหรือไม่

3) พิจารณารูปแบบของข้อมูล



เหมาะสมกับความต้องการหรือไม่

4) พิจารณาความสะดวกในการใช้งาน



ใช้งานง่ายหรือไม่

หลักการเข้าถึงแหล่งข้อมูลดิจิทัล

☞ ที่ตรงกับความต้องการ

1) กำหนดวัตถุประสงค์ในการค้นหาข้อมูล



ว่าต้องการข้อมูลประเภทใด ต้องการข้อมูลเพื่อวัตถุประสงค์ใด

2) กำหนดคำค้นที่เหมาะสม ก ว ค

คำค้นที่ดีควรเป็นคำที่สั้น กระชับ และตรงประเด็น หรืออาจจะใช้คำที่หลากหลายขึ้นหากคำเดียวแล้วไม่พบร

3) เลือกใช้เครื่องมือค้นหาอย่างมีประสิทธิภาพและเจาะจง

เช่น ใช้ Google ค้นหาแบบทั่วไปหรือผ่านรูปภาพ และใช้ YouTube ค้นหา VDO

4) ใช้เครื่องมือค้นหาแบบขั้นสูง

เช่น ค้นหาข้อมูลตามช่วงเวลา ค้นหาข้อมูลตามภาษา

5) พิจารณาความน่าเชื่อถือและตรวจสอบ

ความถูกต้องของข้อมูลก่อนนำไปใช้

โดยพิจารณาจากแหล่งที่มาของข้อมูล เนื้อหาของข้อมูล รูปแบบการนำเสนอข้อมูล เป็นต้น

6) ติดตามข่าวสารจากแหล่งข้อมูลที่น่าเชื่อถือ

ทันสมัยและทันเหตุการณ์

ติดตาม





ธรรมชาติของสื่อ

สื่อเป็นเครื่องมือสำคัญในการถ่ายทอดข่าวสาร ข้อมูล และความรู้ไปยังผู้รับสาร สื่อมีบทบาทสำคัญต่อสังคม ทั้งในด้านการรับรู้ข่าวสาร เสริมสร้างความรู้ความเข้าใจ และการสร้างค่านิยมความเชื่อใจธรรมชาติของสื่อ จึงเป็นสิ่งสำคัญสำหรับผู้คนในยุคปัจจุบัน

ประเภทของธรรมชาติของสื่อ

สามารถแบ่งออกเป็น 5 ประเภท

1 สื่อ คือ สิ่งที่ถูกสร้างขึ้นมาจากมนุษย์

อาศัยความเชื่อและทัศนคติของผู้สร้าง จึงสามารถมีความล้ำเอียง หรืออคติได้ เช่น โฆษณาหรือสินค้าที่เกินจริง การนำเสนอข่าว ที่เอื้อต่อกลุ่มผู้มีอำนาจ เป็นต้น





2 สื่อส่วนใหญ่ที่มีเป้าหมายธุรกิจ

จะมีวัตถุประสงค์เพื่อหารายได้ เน้นดึงดูด ความสนใจผู้คน การที่สื่อมีเป้าหมายแบบนี้ เราต้องตระหนักรว่า มันเป็นสื่อเพื่อความบันเทิง อาจจะวัดเรื่องความถูกต้องหรือเป็นกลางไม่ได้ เช่น โฆษณา รายการเกมโชว์

3 สื่อสร้างค่านิยมและอุดมคติ

ตระหนักไว้เสมอว่าสื่ออาจส่งผลต่อความคิด และพฤติกรรมของเรา เช่น Soft Power ที่เกิดจากอุตสาหกรรมความบันเทิง (ภาพยนตร์ ละครโทรทัศน์ เพลง) เป็นต้น



4 สื่อกำให้เกิดผลกระทบการเมืองและสังคม



สื่อจึงอาจถูกใช้เป็นเครื่องมือในการโฆษณาชวนเชื่อ หรือสร้างความแตกแยกในสังคม เราจึงควร ใช้วิจารณญาณในการรับชมสื่อ เช่น ในช่วงเลือกตั้ง สื่อบางสื่ออาจถูกใช้เป็นเครื่องมือในการปลุกปั่น แพร่กระจายข้อมูลที่เข้าข้างพระคราธรรมเมือง หรือ ข้อมูลที่เป็นเท็จ เพื่อหวังผลทางการเมือง

5

สื่อมีเอกลักษณ์และข้อจำกัดเฉพาะตัว

สื่อบางประเภทอาจนำเสนอข้อมูลได้ละเอียดและรอบด้าน บางประเภทอาจจะเน้นความรวดเร็วเป็นหลัก การเข้าใจเอกลักษณ์นี้จะทำให้เราเลือกรับสื่อได้อย่างเหมาะสม เช่น

- สื่อประเภทสิ่งพิมพ์ จะใช้เทคนิคทางคอมพิวเตอร์เพื่อปรับแต่งภาพใหม่ให้งดงาม หรือใช้คำที่สร้างอารมณ์ความรู้สึก
- สื่อประเภทภาพยนตร์ ละครทีวี หนัง จะใช้การตัดต่อภาพ เสียง แสงไฟ มุกกล้อง Effect ต่าง ๆ สร้างความสมจริงหรือเหนือจริง ?
- สื่อโซเชียลเน็ตเวิร์กจะเน้นที่ความแปลกใหม่ของเรื่องราว หรือเนื้อหา มีความสด ทันต่อกระแสสังคม แต่ไม่ละเอียดลึกซึ้ง



การประเมินคุณภาพ และความน่าเชื่อถือของข้อมูล จากสื่อดิจิทัล

สื่อดิจิทัลมีบทบาทสำคัญในการเผยแพร่ข้อมูลข่าวสารต่าง ๆ ทำให้เราสามารถเข้าถึงข้อมูลข่าวสารได้อย่างรวดเร็ว และสะดวกมากขึ้น แต่สื่อดิจิทัลก็ยังมีความเสี่ยง เกี่ยวกับข้อมูลที่เป็นเท็จหรือบิดเบือนความจริง หรือที่เรารู้จักกันในชื่อ “ข่าวปลอม หรือ Fake News” ดังนั้น การประเมินคุณภาพและความน่าเชื่อถือของข้อมูลจากสื่อดิจิทัล จึงเป็นสิ่งที่สำคัญ

ปัจจัยที่ใช้พิจารณา การประเมินคุณภาพ/ความน่าเชื่อถือของข้อมูล

1 แหล่งที่มาของข้อมูล

มีการระบุชื่อและที่อยู่ของแหล่งที่มาอย่างชัดเจน สามารถตรวจสอบได้ มีประวัติการเผยแพร่ข้อมูลที่เป็นจริง

2 เนื้อหาของข้อมูล

การเป็นเนื้อหาที่มีความถูกต้อง ครบถ้วน มีแหล่งอ้างอิงนำเสนออย่างเป็นกลาง ไม่มีลักษณะอคติหรือชี้นำ ใช้ภาษาถูกต้องเหมาะสม

3 รูปแบบการนำเสนอข้อมูล



ต้องมีความเข้าใจง่าย ไม่ซับซ้อน มีการจัดระเบียบข้อมูลอย่างเป็นระบบ

4 ปฏิกิริยาของผู้คน



หากข้อมูลได้รับความสนใจจากคนจำนวนมาก ในเชิงบวกแสดงว่าข้อมูลนั้นมีความน่าเชื่อถือมากขึ้น

5 ความถี่ของการเผยแพร่ข้อมูล



หากข้อมูลมีการเผยแพร่ซ้ำ ๆ จากแหล่งที่มาที่แตกต่างกันแสดงว่าข้อมูลนั้นมีความน่าเชื่อถือมากขึ้น

รู้เท่ากัน Fake News

ป้องกันความเสี่ยงจากสื่อดิจิทัล



Fake News คืออะไร ?

REMEMBER

คำว่า Fake News ไม่ได้หมายถึงข่าวที่ไม่จริงเท่านั้น แต่ยังรวมถึง ข้อมูลต่าง ๆ ที่ไม่เป็นความจริงด้วย

Claire Wardle จาก First Draft

ซึ่งเป็นองค์กรทำงานต่อต้านข่าวลวงและข้อมูลเท็จเพื่อสร้างความไว้วางใจ และความจริงในยุคดิจิทัล ระบุว่า การที่จะเข้าใจระบบนิเวศของการส่งต่อ หรือแชร์ข้อมูลข่าวสารผิด ๆ ออกไปนั้น ควรจะ ต้องทำความเข้าใจกับ ประเภทของข่าวสารข้อมูลเท็จ แรงจูงใจของคนทำและการแพร่กระจาย ของเนื้อหา



ลักษณะของ Fake News

1



มีเนื้อหาที่เกินจริง
หรือบิดเบือนความจริง

2



สร้างความตื่นตระหนก
หรือสร้างความแตกแยก

3



เล่นกับความรู้สึก

4



มีการเผยแพร่ผ่าน
สื่อสังคมออนไลน์เป็นหลัก

ข้อมูลเท็จมาจากไหน ?

มาจากหลากหลายแหล่ง เช่น

- **佯มุ่งเจตนา :** จะใจให้ข้อมูลเท็จ หรือให้ข้อมูลเท็จโดยรู้เท่าไม่ถึงการณ์
- **佯มุ่งเหตุผลเบื้องหลัง :** ทำเพื่อเงิน เพื่อชื่นนำ เพื่อความสนุก หรือ เพราะความหวังดีที่ขาดความรู้

- แรงมุ่นความถูกต้อง : คาดเคลื่อนทั้งหมด หรือคาดเคลื่อนบางส่วน
- แรงมุ่นกรอบเวลา : ข้อมูลเก่า ข้อมูลใหม่ ข้อมูลที่เป็นจริงในอดีต
- แรงมุ่นแหล่งกำเนิด : ปากต่อปาก ไลน์ เฟซบุ๊ก โซเชียลมีเดียต่าง ๆ

องค์การอนามัยโลก ได้บัญญัติศัพท์อุกมาใช้สื่อถึงการระบาดของข้อมูล ข่าวสารที่ไม่ถูกต้อง คลาดเคลื่อนหรือบิดเบือนเกี่ยวกับโรคติดเชื้อไวรัส โคโรนา คือคำว่าการแพร่ระบาดของข่าวสาร หรือ “Infodemic” เป็นการรวมคำสองคำเข้าด้วยกันจาก Information (ข่าวสาร) และคำว่า Epidemic (การระบาด) โดยข้อมูลในลักษณะนี้ถือเป็นความผิดปกติ ของข้อมูลข่าวสาร (Information Disorder)

นอกจากนี้สหภาพยูโรปยังได้ขยายความ Information Disorder ออกเป็น 3 ประเภท ได้แก่

1 **Misinformation** หรือข้อมูลที่ผิด



2 **Disinformation** หรือข้อมูลบิดเบือน



3 **Malinformation** หรือข้อมูลที่แฝงเจตนาร้าย



ประเภทของข้อมูลเท็จ

ข่าวปลอม (Fabricated Content)

- 1 กุเรื่องมั่วทั้งหมด มุ่งหลอกลวง



ชี้นำ (Misleading Content)

- 2 จัดฉากข้อมูลเพื่อชี้นำ ใส่ร้าย



โยงมั่ว (False Connection)

- 3 ไม่สัมพันธ์กันระหว่างพادหัว ภาพ คลิป หรือคำบรรยาย ประกอบ



ผิดบริบท (False Context)

- 4 เป็นข้อมูลจริง แต่นำมาใช้ผิดบริบท



ล้อเลียน (Satire & Parody)

- 5 เนื้อหาเสียดสีให้เกิดความตลกขบขัน ไม่มุ่งให้เกิดอันตราย แต่อาจทำให้บางคนหลงเชื่อว่าเป็นความจริง



สวมรอย (Imposter Content)

- 6 ปลอมตัวสวมรอยให้ข้อมูล เพื่อหลอกลวงหรือหวังร้าย



หลอกลวง (Manipulated Content)

- 7 สร้างแต่งตัดข้อมูล เพื่อหลอกลวงโดยเฉพาะ



สาเหตุที่มาของข้อมูลเท็จ



1. การขาดทักษะความรู้เท่าทัน การเผยแพร่ และวิเคราะห์ข่าว หรือสารสนเทศอื่น ๆ
2. ต้องการปลูกปั้นยุยง
3. ข้อมูลเลือกข้าง
4. เพื่อชี้นำทางการเมือง
5. ความต้องการเสียดสีเพื่อความชอบชั้น
6. เพื่อสนองความพึงพอใจ
7. เพื่อสร้างรายได้
8. เพื่อโฆษณาชวนเชื่อ

การตรวจสอบเบื้องต้น

1 ตรวจสอบแหล่งที่มาของข่าวสารข้อมูล

เช่น สำนักข่าว หน่วยงาน ชื่อผู้ให้ข้อมูลมีความน่าเชื่อถือ เป็นต้น

2 ตรวจสอบแหล่งข้อมูลอื่น ๆ ประกอบ

เช่น หน่วยราชการหรือหน่วยงานที่น่าจะเกี่ยวข้องกับข่าวสารข้อมูลนั้น ๆ เพื่อยืนยันว่ามีเรื่องหรือเหตุการณ์ดังกล่าวจริง

3 ตรวจสอบหาต้นต่อของข่าว

บางครั้งข่าวเท็จอาจเป็นข่าวเก่าที่เคยเกิดขึ้นแล้วหรือใช้ข้อมูลจากข่าวเก่ามาเล่าใหม่ เพื่อให้เกิดความแตกตื่นหรือเพื่อประโยชน์แอบแฝง

4 ส观音ผู้เชี่ยวชาญในเรื่องนั้น ๆ โดยตรง

หรือหากข้อมูลเพิ่มเติมจากแหล่งที่เชื่อถือได้

สาเหตุที่มาของข้อมูลเท็จ

คำแนะนำในการรับมือกับข่าวปลอม

1. อาย่าเชื่อข้อมูลที่เห็นหรือได้ยินในทันที



2. ตรวจสอบแหล่งที่มาของข้อมูล ก่อนจะกดแชร์หรือเผยแพร่



3. ใช้วิจารณญาณในการรับข้อมูล



4. หากพบเห็นข่าวปลอม ควรรายงานไปยังหน่วยงานที่เกี่ยวข้อง



ทั้งนี้บางครั้งคนก็เผยแพร่เนื้อหาอกไปโดยไม่รู้ว่า เป็น Misinformation ที่ข้อมูลผิดหรือถูกบิดเบือน เพียงเพราะความประณานดีต่อสังคมดิจิทัล

แนวทางในการรับชมสื่อ อย่างรู้เท่าทัน



การเข้าใจธรรมชาติของสื่อ จะช่วยให้เราสามารถรับชมสื่อได้อย่างรู้เท่าทัน เราสามารถวิเคราะห์เนื้อหาของสื่อได้อย่างมีวิจารณญาณ และเรามาสามารถเลือกรับสื่อที่เป็นประโยชน์ต่อตนเองและสังคม

แนวทางในการรับชมสื่อย่างรู้เท่าทัน มีดังนี้

1 ตระหนักถึงธรรมชาติของสื่อ

ก่อนรับชมสื่อใด ๆ ควรตระหนักถึงธรรมชาติของสื่อนั้น ๆ ว่า สื่อนั้นถูกสร้างขึ้นโดยใคร มีเป้าหมายอย่างไร และอาจส่งผลอย่างไรต่อตนเองและสังคม



2 ตรวจสอบแหล่งที่มาของข้อมูล

ก่อนเชื่อข้อมูลใด ๆ ที่ได้รับจากสื่อ ควรตรวจสอบแหล่งที่มาของข้อมูลว่าเชื่อถือได้หรือไม่

3 ใช้วิจารณญาณในการรับชมสื่อ

ไม่ควรเชื่อข้อมูลของสื่ออย่างทันที ควรใช้วิจารณญาณในการตีความข้อมูลและพิจารณาว่าข้อมูลนั้นสอดคล้องกับความเป็นจริงหรือไม่



4 ไม่ควรรับชมสื่อจากแหล่งเดียว

ควรรับชมสื่อจากแหล่งต่าง ๆ ที่หลากหลาย เพื่อให้ได้มุมมองที่หลากหลาย

5 มีส่วนร่วมในการแลกเปลี่ยนข้อมูล

เราสามารถมีส่วนร่วม ในการแลกเปลี่ยนข้อมูล กับผู้อื่น เพื่อแลกเปลี่ยนมุมมองและความคิดเห็น เกี่ยวกับสื่อต่าง ๆ





ศิลปะแห่งการจัดการข้อมูลจากสื่อดิจิทัล ด้วยตนเอง

การให้ความสำคัญกับข้อมูลส่วนบุคคล ข้อมูลการทำงาน และข้อมูลที่เกี่ยวข้องกับความสำเร็จของกิจกรรมต่าง ๆ เป็นบทบาทที่สำคัญในการบริหารชีวิตที่มีประสิทธิภาพ

**มาสำรวจแนวทาง และแลกเปลี่ยนประสบการณ์ใน
การจัดการข้อมูล ด้วยตนเองกัน !**

1 กำหนดและบริหารข้อมูลส่วนบุคคล

ก่อนรับชมสื่อใด ๆ ควรตระหนักรู้ถึงธรรมชาติของสื่อนั้น ๆ ว่า สื่อนั้นถูกสร้างขึ้นโดยใคร มีเป้าหมายอย่างไร และอาจส่งผลอย่างไรต่อตนเอง และสังคม

2 ใช้เทคโนโลยีเพื่อจัดการข้อมูล

โดยใช้แอปพลิเคชันหรือเทคโนโลยีต่าง ๆ ช่วย

3 การจัดหมวดหมู่ และสร้างระบบข้อมูล

ใช้ชื่อไฟล์และโฟลเดอร์ที่ชัดเจน และการสร้างระบบที่เข้าใจง่ายช่วยให้ค้นหาข้อมูลเป็นเรื่องง่าย

4 การสำรวจและลบข้อมูลที่ไม่จำเป็น

ทุก ๆ ครั้งที่ได้รับข้อมูลเพิ่มมากขึ้น ควรทำการตรวจสอบ และลบข้อมูลที่ไม่จำเป็นออก

5 การสร้างนิสัยการสำรวจและปรับปรุง

เราสามารถมีส่วนร่วมในการแลกเปลี่ยนข้อมูลกับผู้อื่น เพื่อแลกเปลี่ยนมุมมองและความคิดเห็นเกี่ยวกับสื่อต่าง ๆ

6 การทำสำเนาข้อมูล (Backup)

การทำสำเนาข้อมูลเป็นการป้องกันการสูญเสียข้อมูลที่สำคัญ เช่น ทำสำเนาในระบบคลาวด์ (Cloud)

7 การปฏิบัติตามกฎหมายและนโยบาย

การทราบถึงนโยบายความเป็นส่วนตัวของบริษัทที่ให้บริการ และการปฏิบัติตาม ช่วยลดความเสี่ยงที่อาจเกิดขึ้น

8 การเรียนรู้เพิ่มเติมเกี่ยวกับเทคโนโลยีและเครื่องมือใหม่ ๆ

ที่มีความสามารถในการจัดการข้อมูล จะช่วยเพิ่มประสิทธิภาพในการจัดการข้อมูล

ผลจากการแบ่งปัน

เนื้อหาที่ไม่เหมาะสม

อินเทอร์เน็ตได้กลายเป็นสื่อหลักในการรับสาร และสื่อสารของคนทั่วโลก ส่งผลให้ปริมาณข้อมูลบนอินเทอร์เน็ตมีจำนวนมหาศาล มีทั้งข้อมูลที่ดี และมีประโยชน์ต่อสังคม ขณะเดียวกัน ก็มีข้อมูลที่ไม่เหมาะสมอยู่เป็นจำนวนมาก

ข้อมูลที่ไม่เหมาะสม

ในที่นี้หมายถึง ข้อมูลใด ๆ ที่ขัดต่อกฎหมาย ศีลธรรม หรือจริตประเพณี ของสังคม เช่น เนื้อหาลามกอนาจาร เนื้อหาที่สร้างความแตกแยกหรือ เกลียดชัง เนื้อหาที่เผยแพร่ข้อมูลเท็จหรือบิดเบือนความจริง เป็นต้น

ผลกระทบจากการแบ่งปันเนื้อหาที่ไม่เหมาะสม

01

สร้างความเสียหายต่อบุคคลอื่น



เนื้อหาที่ไม่เหมาะสมบางประเภทอาจสร้างความเสียหาย ต่อบุคคลอื่น เช่น เนื้อหาลามกอนาจาร อาจทำให้ บุคคลอื่นรู้สึกอับอายหรือถูกกลั่นเมิด เนื้อหาที่สร้างความแตกแยก หรือเกลียดชังอาจทำให้บุคคลอื่นรู้สึกเกลียดชัง หรือถูกรังแก เป็นต้น

EXAMPLE



ตัวอย่างที่เห็นได้ชัด เช่น

- กรณีนำภาพของบุคคลไปเผยแพร่โดยไม่ได้รับอนุญาต หรือ การนำภาพหรือวิดีโอลามกอนาจารของบุคคล ไปเผยแพร่ ซึ่งอาจทำให้บุคคลนั้นรู้สึกอับอาย หรือถูกกลั่นเมิด ในการณ์ที่ รุนแรงอาจนำไปสู่การข่าตัวตายได้
- กรณีที่มีการเผยแพร่ข้อความ หรือเนื้อหาที่สร้างความ แตกแยกหรือเกลียดชัง ซึ่งอาจทำให้บุคคลอื่น รู้สึกถูก เกลียดชัง หรือถูกรังแก

EXAMPLE

จับแล้วหนุ่มหลอกเด็ก 17 ถ่ายคลิปไปแบล็กเมลรีดเงิน

SCAN
ME!

รวบแล้วหนุ่มแสบหลอกนักเรียนชายวัย 17 ปี ถ่ายคลิปไป แล้วแบล็กเมลรีดเงินหลายครั้งจนเด็กคิดสั้น พบประวัติ ก่อเหตุ โขกโชน มีผู้ตกเป็นเหยื่อเกือบ 20 ราย

EXAMPLE

ผู้ต้องหารับสารภาพว่า ใช้วิธีปลอมໂປຣໄຟລ໌ໃນອິນສຕາແກຣມ ເປັນ ກາພທຸງສາວໜ້າຕາດີແລະໄປຫາເຫັນໃນແຊຕລັບຫາຄູ່ ຈົນພບກັບ ເຫັນເມື່ອມີປາຍເດືອນມកຣາມທີ່ຜ່ານມາ ຈຶ່ງແຊຕຕີສົນທ ພູດຄຸຍ ທລອກລ່ອຊັກຂວານຂອມມີເພັສສັມພັນຮັບ ແຕ່ຂອໃຫ້ເຫັນຄ່າຍຄລິປຽບປ່າງ ໂປ່ປັບລືອມໄທດູກ່ອນ ເມື່ອເຫັນຫລັງເຂົ້ອ ຈຶ່ງຂໍມູຽດໄດ້ເຈີນ ຄວັງລະ 4,000-5,000 ບາທ ໄນເຫັນນັ້ນຈະແພຍແພຣ່ກາພຄລິປີໃນໂຫເຊີລ ໄດ້ເຈີນໄປກວ່າ 20,000 ບາທ ຈົນເມື່ອວັນທີ 13 ມີນາມທີ່ຜ່ານມາ ໄດ້ຂໍມູ່ເຫັນຂອງເຈີນອີກ 20,000 ບາທ ຈົນເຫັນເກີດຄວາມເຄີຍດ ໃຫ້ຈາກຮັບປິດຂອງພ່ອປລິດຊື່ພັດວັນ

02**สร้างความเสียหายต่อสังคมโดยรวม**

เนื้อหาທີ່ໄຟເໜາສົມ ອາຈສ້າງຄວາມເສີຍຫາຍຕ່ອສັງຄົມ ໂດຍຮັມ ເຊັ່ນ ເນື້ອຫາທີ່ແພຍແພຣ່ຂໍ້ມູນເຖິງ ທີ່ຮົ່ວບົດເບືອນ ຄວາມຈົງຈາກທຳໃຫ້ສັງຄົມເກີດຄວາມສັບສນແລະແຕກແຍກ ເນື້ອຫາທີ່ສັ່ງເສີມຄວາມຮຸນແຮງ ອາຈທຳໃຫ້ສັງຄົມເກີດຄວາມ ວຸ່ນວາຍແລະອາຊຸງກາຮົມ ເປັນຕົ້ນ

EXAMPLE

ตัวอย่างที่เห็นได้ชัด เช่น



กรณีที่มีการนำข่าวปลอมไปเผยแพร่ ซึ่งอาจทำให้ประชาชนเกิดความสับสนและแตกแยก เช่น

- การนำข่าวปลอมเรื่องการแพร่ระบาดของโรคระบาดไปเผยแพร่ ซึ่งอาจทำให้ประชาชนเกิดความตื่นตระหนกและกักตุนสินค้า
- การนำข่าวปลอมเรื่องการเลือกตั้งไปเผยแพร่ ซึ่งอาจทำให้ประชาชนเกิดความแตกแยกและนำไปสู่ความรุนแรงได้
- กรณีที่มีการนำภาพหรือวิดีโอความรุนแรง ไปเผยแพร่ ซึ่งอาจทำให้สังคมเกิดความหวาดกลัว และอาจนำไปสู่การส่งเสริมความรุนแรง เช่น การนำภาพหรือวิดีโอการฆ่าตัวตายไปเผยแพร่ ซึ่งอาจทำให้เยาวชนเกิดความคิดที่จะฆ่าตัวตายได้

03

ส่งผลกระทบต่อผู้แบ่งปันเนื้อหา



ผู้แบ่งปันเนื้อหาที่ไม่เหมาะสม อาจถูกดำเนินคดีทางกฎหมายหรือถูกสังคมประณาม เช่น หากแบ่งปันเนื้อหาลามกอนาจาร อาจถูกดำเนินคดีฐานผลิตหรือเผยแพร่สื่อสารลามกอนาจาร หากแบ่งปันเนื้อหาที่สร้างความแตกแยกหรือเกลียดชัง อาจถูกดำเนินคดีฐานยุยงปลุกปั่น หากแบ่งปันเนื้อหาที่เผยแพร่ข้อมูลเท็จ หรือบิดเบือนความจริง อาจถูกดำเนินคดีฐานหมิ่นประมาท เป็นต้น

ดังนั้น จึงควรระมัดระวังในการแบ่งปันเนื้อหาบนอินเทอร์เน็ต ตรวจสอบให้แน่ใจว่าเนื้อหาที่แบ่งปันนั้นไม่เหมาะสมต่อผู้อื่นหรือสังคมโดยรวม หากพบเห็นเนื้อหาที่ไม่เหมาะสม ควรแจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อดำเนินการจัดการอย่างเหมาะสม

มาดูกันว่า การใช้งานหรือ
เผยแพร่ข้อมูลใดบ้าง ที่ทำบันโลกดิจิทัล^๑
แล้วขัดต่อกฎหมาย หรือขัดต่อจริยธรรม



การกระทำ/พฤติกรรม 	ผลกระทบ ทางกฎหมาย 	ผลกระทบ ทางธุรกิจ 
ฝ่ากร้าน ขายของ และส่งข้อความก่อการ โดยไม่ได้รับอนุญาต หรือผู้รับปฏิเสธไม่ได้	มีความผิดปรับไม่เกิน 2 แสนบาท	ทำให้ผู้อื่น เกิดความรำคาญ
โพสต์ หรือแชร์ข้อมูลเท็จ ที่สร้างความเสียหาย ต่อบุคคล หรือประเทศ	จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสน และระงับข้อมูลนั้น	เกิดความเข้าใจผิด อับอาย สร้างความเกลียดชัง ทำให้เสื่อมเสียชื่อเสียง
โพสต์ข้อมูลปลอม ทุจริต หลอกลวงสร้างความเสียหาย ด้านความมั่นคง	จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสน และระงับข้อมูลนั้น หรือ บทลงโทษตามมาตรา ที่เกี่ยวข้อง	เกิดความตื่นตระหนก การขัดแย้งทางสังคม ทำให้การตัดสินใจ ผิดพลาดได้
โพสต์ หรือแชร์ข้อมูล ภาพดัดต่อ ที่สร้างความเสื่อมเสียต่อผู้อื่น รวมถึงผู้เสียชีวิต	จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 2 แสน และระงับข้อมูลนั้น	สร้างความอึดอัดใจ ความสะเทือนใจ และความรู้สึกหลอนใจ

การกระทำ/พฤติกรรม 	ผลกระบก ทางกฎหมาย 	ผลกระบก ทางจริยธรรม 
โพสต์หรือแชร์ภาพเป็น เปลือย ลามกอนาจาร การพนัน	จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 1 แสน หรือทั้งจำทั้งปรับ และระงับข้อมูลนั้น	ทำให้ผู้อื่นเกิดความวิตก กังวล อับอาย เสียชื่อเสียง
โพสต์ แชร์ หรือขาย โปรแกรม เพลง ภาพพนัน โดยไม่ได้รับอนุญาต	ความผิดด้านลิขสิทธิ์ จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 2 หมื่น หรือทั้งจำทั้งปรับ	ถือเป็นการขโมย ลักทรัพย์ ทำให้ผู้อื่นเสียผลประโยชน์
การส่งข้อความทำธุรกรรมทางการเงิน เช่น แชตมิลเจน ถือเป็นหลักฐาน หรือสัญญาทางการเงิน	หากไม่คืนหรือทำตาม ข้อตกลง เจ้าหนี้ฟ้องร้อง ทางแพ่ง เพื่อเรียกเงินคืนได้ ตาม พ.ร.บ. ธุรกรรม ทางอิเล็กทรอนิกส์	ทำให้ผู้อื่นเกิดความเดือดร้อน ไม่สบายใจ วิตกกังวล กลัวว่าจะเสียทรัพย์
การกด Like กด Share ถือเป็นการเผยแพร่ข้อมูล หากข้อมูลนั้นเป็นข้อมูล ปลอม เท็จ นั่นเท่ากับว่า เราผิดกฎหมาย พ.ร.บ. แล้ว	จำคุกไม่เกิน 5 ปี หรือ ปรับไม่เกิน 1 แสน หรือ ทั้งจำทั้งปรับ	ทำให้ผู้อื่นเกิดความไม่สบายใจ เสื่อมเสียชื่อเสียง



รู้เท่าทันใช้ข้อมูลอย่างปลอดภัย
 คลายสงสัยให้สีบค้นต้นแหล่งศูนย์
 ให้ใช้หลักการเข้าถึงช่วยเกือกภูล
 จะเพิ่มพูนความรู้จักทักษะ praw
 กำหนดวัตถุประสงค์ใส่คำค้น
 ใช้เครื่องมือมากล้านสนใจข่าว
 ต้องระวังข้อมูลเท็จแชร์เรื่องราว
 ควรสีบสาวก่อนใช้ดูให้ดี

ถ้าคุณเรียนผ่านด้านนี้
คุณจะสร้างสื่อได้ปังและโดนใจ
ไม่เสียงทำผิดกฎหมายด้านลิขสิทธิ์
ที่มีโทษสูงทั้งจำและปรับ



5.2

DIGITAL CONTENT CREATION

วัตถุประสงค์

- ผู้เรียนสามารถอธิบายวิธีการสร้างเนื้อหา หรือสื่อดิจิทัลสอดคล้องกับวัตถุประสงค์ในการนำไปใช้และประเด็นกฎหมายที่เกี่ยวข้อง เช่น ลิขสิทธิ์สัญญาอนุญาตแบบเปิด (CREATIVE COMMONS) ได้
- ผู้เรียนสามารถเข้าใจถึงการผลิต หรือสร้างสรรค์เนื้อหาหรือสื่อดิจิทัลที่สอดคล้องกับวัตถุประสงค์ ให้เกิดประโยชน์ในการนำไปใช้และสังคมได้
- ผู้เรียนสามารถตระหนักรถึงจรรยาบรรณในการทำงาน หรือเนื้อหาของผู้อื่นมาใช้ในการสร้างสรรค์เป็นผลงานของตนเองได้



สื่อและเนื้อหาดิจิทัล



สื่อและเนื้อหาดิจิทัลมีบทบาทสำคัญในชีวิตประจำวันของเรา ทั้งด้านการสื่อสาร การศึกษา ความบันเทิง และธุรกิจ สื่อและเนื้อหาดิจิทัลมีรูปแบบที่หลากหลาย ขึ้นอยู่กับวัตถุประสงค์ รูปแบบการนำเสนอ และช่องทางการเผยแพร่

ประเภทของสื่อดิจิทัล

แบ่งออกได้เป็น 3 ประเภทหลัก คือ

1. แบบข้อความ (Text-Based Digital Media)

บทความ บล็อก ข่าวสาร อีเมล ข้อความบนโซเชียลมีเดีย

2. แบบภาพ (Image-Based Digital Media)

รูปถ่าย ภาพกราฟิก ภาพวาด อินโฟกราฟิก

3. แบบวิดีโอ (Video-Based Digital Media)

วิดีโอลิป ภาพยนตร์ รายการทีวี สตรีมมิ่ง

ประเภทของเนื้อหาดิจิทัล

เนื้อหาดิจิทัลสามารถแบ่งออกได้ตามวัตถุประสงค์ ดังนี้

1. ด้านการศึกษา (Educational Content)

บทเรียนออนไลน์ คอร์สเรียน วิดีโอสอน หนังสืออิเล็กทรอนิกส์

2. ด้านความบันเทิง (Entertainment Content)

เกม เพลง ภาพยนตร์ รายการทีวี วิดีโอตลก

3. ด้านการสื่อสาร (Communication Content)

อีเมล ข้อความบนโซเชียลมีเดีย วิดีโอกล

4. ด้านธุรกิจ (Business Content)

เว็บไซต์ โฆษณาออนไลน์ อีเมลการตลาด บทความบล็อก

รูปแบบการนำเสนอ ของสื่อและเนื้อหาดิจิทัล

สามารถเผยแพร่ผ่านช่องทางต่าง ๆ มากมาย ขึ้นอยู่กับกลุ่มเป้าหมายและวัตถุประสงค์ ตัวอย่างช่องทางการเผยแพร่ ได้แก่

- เว็บไซต์ 
- แอปพลิเคชัน 
- สื่อสิ่งพิมพ์ดิจิทัล
 เช่น E-book หรือนิตยสารออนไลน์ 
- โซเชียลมีเดีย 
- อีเมล 

ตัวอย่างการใช้งานสื่อและเนื้อหาดิจิทัล

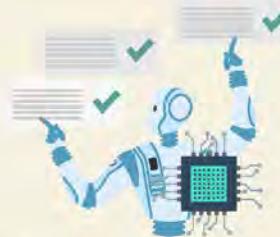
การศึกษา : สามารถเรียนออนไลน์ ผ่านเว็บไซต์ หรือแอปพลิเคชันต่าง ๆ และสามารถใช้สื่อดิจิทัลเพื่อประกอบการสอนได้ เช่น วิดีโอ อินโฟกราฟิก เกม เป็นต้น

ความบันเทิง : สามารถฟังเพลง ดูหนัง เล่นเกม ผ่านแพลตฟอร์มดิจิทัล ต่าง ๆ

การสื่อสาร : สามารถติดต่อสื่อสารกันผ่านโซเชียลมีเดีย แอปพลิเคชัน ส่งข้อความ และโปรแกรมประชุมออนไลน์

ธุรกิจ : สามารถใช้สื่อดิจิทัลเพื่อการโฆษณา ประชาสัมพันธ์ สร้างแบรนด์ และขายสินค้า

แนวโน้มของ สื่อและเนื้อหาดิจิทัล ในอนาคต



- การเติบโตของปัญญาประดิษฐ์ (AI) :
AI จะถูกนำมาใช้เพื่อสร้างและ personalize เนื้อหาดิจิทัล
- การเพิ่มขึ้นของ Virtual Reality (VR) และ Augmented Reality (AR) :
VR และ AR จะสร้างประสบการณ์ที่สมจริงยิ่งขึ้นสำหรับผู้ใช้
- การเติบโตของ Social Media :
Social Media จะเป็นช่องทางหลักในการเผยแพร่เนื้อหาดิจิทัล
- การเพิ่มขึ้นของ Mobile Devices :
ผู้คนจะใช้ Mobile Devices มากขึ้นในการเข้าถึงเนื้อหาดิจิทัล



**สื่อหรือเนื้อหา
ที่เกิดประโยชน์กับสังคม
เป็นอย่างไร ?**

ในยุคดิจิทัลที่ข้อมูลข่าวสาร氾่บ้ำ ผู้คนสามารถเข้าถึงสื่อและเนื้อหาต่าง ๆ ได้อย่างสะดวกรวดเร็ว สื่อจึงมีบทบาทสำคัญในการกำหนดทิศทาง ความคิด และพฤติกรรมของสังคม

สื่อหรือเนื้อหา ที่เกิดประโยชน์กับสังคม

หมายถึง สื่อหรือเนื้อหาที่ส่งผลดีต่อสังคม ช่วยพัฒนาคุณภาพชีวิต และส่งเสริมความเจริญก้าวหน้าในด้านต่างๆ

ลักษณะของสื่อหรือเนื้อหา ที่เกิดประโยชน์กับสังคม

**1 นำเสนอบรรลุข่าวสารที่ถูกต้อง
ครบถ้วนและเป็นกลาง**



- ตรวจสอบข้อเท็จจริงก่อนนำเสนอ
- อ้างอิงแหล่งที่มาของข้อมูล
- นำเสนอเนื้อหาอย่างตรงไปตรงมา ไม่บิดเบือน
- นำเสนอหลายແໜ່ງນຸ້ອງປະເທດ

**2 ส่งเสริมความรู้ ความคิดสร้างสรรค์
และก้าว向社会**



- เนื้อหามีคุณค่า สาระประโยชน์
- กระตุ้นให้คิดวิเคราะห์
- พัฒนาทักษะการคิดสร้างสรรค์
- ส่งเสริมทักษะจำเป็นสำหรับชีวิต

3

สร้างสรรค์สังคมแห่งการเรียนรู้



- กระตุ้นให้ใฝ่รู้ ใฝ่เรียน
- สนับสนุนการศึกษา
- แบ่งปันความรู้
- ส่งเสริมการอ่าน

4

ยกย่องคุณธรรม จริยธรรม และค่านิยมที่ดีงาม



- เนื้อหาสอดคล้องกับค่านิยมที่ดีงาม
- ส่งเสริมความดีงาม
- ยกย่องบุคคลต้นแบบ
- กระตุ้นให้ทำความดี

5

สร้างความสามัคคี ปrongดอง และความเข้าใจในสังคม



- เนื้อหาส่งเสริมความหลากหลาย
- หลีกเลี่ยงการแบ่งแยก
- กระตุ้นการรับฟัง
- ส่งเสริมการอยู่ร่วมกันอย่างสันติ

6

กระตุ้นให้มีส่วนร่วม ในการพัฒนาสังคม



- นำเสนอปัญหาในสังคม
- กระตุ้นให้คิดหาวิธีแก้ไข
- สนับสนุนการมีส่วนร่วม
- ยกย่องการเสียสละ

7

ส่งเสริมความบันเทิง อย่างสร้างสรรค์



- เนื้อหาเหมาะสมกับวัย
- ส่งเสริมจินตนาการ
- พัฒนาทักษะต่าง ๆ
- สร้างความสนุกสนานผ่อนคลาย

บทบาทสำคัญของผู้รับสาร ที่ช่วยให้สื่อหรือเนื้อหาเกิดประโยชน์กับสังคม

- คิดวิเคราะห์ แยกแยะข้อมูล
- ตรวจสอบความถูกต้อง
- เลือกบริโภคสื่อที่มีคุณภาพ
- แบ่งปันเนื้อหาดี ๆ
- ร่วมสร้างสรรค์เนื้อหาที่เป็นประโยชน์

การสร้างเนื้อหาดิจิทัล ให้ดึงดูด และเกิดการจดจำ



ทุกวันนี้การสื่อสาร เทคโนโลยี และไอเดีย ทำให้มีเว็บไซต์สามารถเป็น Content Creator ได้ แต่การที่เราจะกล่าวเป็นคนสร้างเนื้อหาดิจิทัล เราต้องอย่าลืมคิดว่า เมื่อเรามีผู้ติดตาม เราจะกล่าวเป็นคนที่ส่งผลต่อ แนวคิด และมีอิทธิพลต่อลูกเหล่านั้น ดังนั้น ต้องคิดให้ดีกว่าเราจะ นำเสนอเนื้อหาอะไร และอย่างไรจึงจะเหมาะสม

แนวทางการสร้างเนื้อหา ให้ดึงดูด และเกิดการจดจำ

1) วิเคราะห์ให้รู้ว่ากลุ่มเป้าหมาย



สนใจอะไร ต้องการอะไร และสร้างสื่อให้ตรงใจกับกลุ่มเป้าหมาย

2) เลือกหัวข้อที่น่าสนใจ



อาจจะเป็นหัวข้อที่ไม่น่าจะมีครู่มาก่อน หรือนำเสนอແง່ມູນໃໝ່
ที่คาดไม่ถึง

3) เขียนเนื้อหาให้ง่าย กระชับ



เนื่องจากผู้คนมีการจดจ่อ กับสื่อได้สื่อหนึ่งน้อยลงมาก อีกทั้งยังมีสื่อ
อีกจำนวนมากให้เลือกดู หากเข้าใจยากไปคนอาจจะเปลี่ยนไปดูสื่อ
อื่น ๆ แทน

4) ใช้ใจรูปภาพ และวิดีโอ



รูปภาพเป็นส่วนสำคัญที่จะช่วยดึงดูดความสนใจ และสร้างความน่าสนใจให้กับเนื้อหา

5) เน้นการเล่าเรื่อง



สร้างความน่าติดตาม กระตุ้นอารมณ์ สร้างความอินกับเนื้อหา

6) ใส่ความคิดสร้างสรรค์



มีลูกเล่น ไอเดียที่แตกต่าง สร้างจุดขายที่ไม่เหมือนใคร

7) กระตุ้นการมีส่วนร่วม



ตั้งคำถาม ชวนแสดงความคิดเห็นหรือจัดกิจกรรมต่าง ๆ

8) ตรวจสอบความถูกต้อง



ตรวจทานเนื้อหาให้ละเอียดก่อนการเผยแพร่

9) วิเคราะห์ผลลัพธ์



ติดตามผลตอบรับ เพื่อนำมาปรับปรุง

10) พัฒนาอย่างต่อเนื่อง



เรียนรู้เทคนิคและค้นหาแรงบันดาลใจใหม่ ๆ อยู่เสมอ

หลักการสร้างเนื้อหา

ให้ถูกกฎหมาย และมีจริยธรรม



การสร้างเนื้อหาที่มีคุณภาพไม่เพียงให้ความสำคัญกับความน่าสนใจ และคุณค่าที่นำเสนอเท่านั้น แต่ยังต้องพิจารณาถึงจริยธรรม และการไม่ผิดต่อกฎหมายด้วย

หลักการการสร้างเนื้อหาอย่างมี จริยธรรม และไม่ผิดกฎหมาย

- ชื่อสัตย์ต่อผู้ชม ไม่บิดเบือนข้อมูล
เพื่อให้ได้รับความสนใจ



- เคารพลิขสิทธิ์และทรัพย์สินทางปัญญา
ไม่แอบอ้างเอาผลงานของผู้อื่นมาเป็นของตัวเอง



- รับผิดชอบต่อสังคม



- ป้องกันข้อมูลส่วนบุคคลของทุกคนที่เกี่ยวข้อง



- ตรวจสอบข้อเท็จจริงก่อนเผยแพร่เนื้อหา



ให้เครดิตหรืออ้างอิงที่เหมาะสม

- ไม่ละเมิดลิขสิทธิ์ผู้อื่น หากมีส่วนที่นำเนื้อหา
ของผู้อื่นมาใช้งาน



- หลักเลี่ยงเนื้อหาที่ก่อให้เกิดความขัดแย้ง
หรือปลุกระดม



แนวทางปฏิบัติ

1

ตรวจสอบข้อมูลก่อนนำมาเผยแพร่ :

ตรวจสอบความถูกต้องของข้อมูล แหล่งที่มา และความน่าเชื่อถือ หลีกเลี่ยงการเผยแพร่ข่าวลือ ข้อมูลเท็จ หรือข้อมูลที่บิดเบือน

2

อ้างอิงแหล่งที่มาของข้อมูล :

ระบุแหล่งที่มาของข้อมูลอย่างชัดเจน เพื่อให้ผู้อื่นสามารถตรวจสอบข้อมูลย้อนหลังได้

3

ระบบชี้อผู้สร้างเนื้อหา :

ระบบชี้อผู้สร้างเนื้อหา ช่องทางการติดต่อ และข้อมูลอื่น ๆ ที่เกี่ยวข้อง

4

หลีกเลี่ยงการใช้ภาษาที่รุนแรงหรือไม่เหมาะสม :

ใช้ภาษาสุภาพ เนมานะสมกับกลุ่มเป้าหมาย หลีกเลี่ยงการใช้คำหยาบคาย ภาษาที่แสดงความเกลียดชังหรือภาษาที่สร้างความเสียหาย

5

คิดวิเคราะห์และไตรตรองก่อนแชร์ต่อ :

ตรวจสอบเนื้อหา ความถูกต้อง และความน่าเชื่อถือ ก่อนที่จะแชร์ต่อ

การณีศึกษา

1

การเผยแพร่ข่าวลือ : การเผยแพร่ข้อมูลเท็จหรือปิดเบี่ยงความจริงอาจสร้างความเสียหายต่อบุคคลอื่นหรือสังคม

ตัวอย่างเช่น การเผยแพร่ข่าวลือเกี่ยวกับสถานการณ์โรคระบาดอาจสร้างความตื่นตระหนกและความหวาดกลัว

2

การละเมิดลิขสิทธิ์ : การนำผลงานของผู้อื่นมาใช้โดยไม่ได้รับอนุญาตเป็นการละเมิดลิขสิทธิ์

ตัวอย่างเช่น การนำรูปภาพจากเว็บไซต์มาใช้โดยไม่ได้ขออนุญาต

3

การปลุกระดมความเกลียดชัง : การโพสต์ข้อความหรือรูปภาพที่สร้างความเกลียดชัง แบ่งแยก หรือดูหมิ่นบุคคลอื่น

ตัวอย่างเช่น การโพสต์ข้อความที่แสดงความเกลียดชังต่อบุคคลต่างศาสนา

ตัวอย่างเครื่องมือและแหล่งข้อมูล

- Creative Commons :

องค์กรที่จัดทำสัญญาอนุญาตแบบเปิด ช่วยให้ผู้สร้างเนื้อหาสามารถกำหนดเงื่อนไขการใช้ผลงาน

- เว็บไซต์ของกรมทรัพย์สินทางปัญญา :

ให้ข้อมูลเกี่ยวกับกฎหมายและวิธีการจดทะเบียนลิขสิทธิ์
[\(https://www.ipthailand.go.th/\)](https://www.ipthailand.go.th/)

- เว็บไซต์ของสำนักงานคณะกรรมการกฤษฎีกา :

ให้ข้อมูลเกี่ยวกับกฎหมายไทย (<https://ocs.go.th/>)



ลิขสิทธิ์ กับ CREATIVE COMMONS

เรารู้จักลิขสิทธิ์ดีแค่ไหน ?

สื่อและเนื้อหาทุกอย่างล้วนมีลิขสิทธิ์ เราไม่สามารถนำมาใช้ได้ โดยไม่ขออนุญาตจากเจ้าของ การ Repost อาจดูเป็นการโพสต์ธรรมดายิบเรื่องเก่านำมาโพสต์ใหม่ เพื่อให้ผู้ติดตามหรือคนอื่น ๆ ที่ไม่เคยเห็นได้เห็น เป็นการแพร่เรื่องราวดี ๆ ใหม่อีกรอบ แต่ถ้าเราไม่ใช่คนที่คิดหรือสร้างเนื้อหานั้นขึ้นมาเอง ก็อาจกล่าวเป็นเรื่องของการละเมิดสิทธิ์ของคนอื่นได้

ประเภทของงานมีลิขสิทธิ์

งานอันมีลิขสิทธิ์ มี 9 ประเภท ได้แก่

1) งานวรรณกรรม



เช่น หนังสือ บทความ บทกลอน โปรแกรมคอมพิวเตอร์ เป็นต้น

2) นาฏกรรม



เช่น ท่าเต้น ท่ารำ ที่ประกอบขึ้นเป็นเรื่องราว เป็นต้น

3) ศิลปกรรม



เช่น ภาพวาด ภาพถ่าย เป็นต้น

4) ดนตรีกรรม



เช่น ทำนองเพลง หรือเนื้อร้อง และทำนองเพลง เป็นต้น

5) โซตักันวัสดุ



เช่น คอมพิวเตอร์พร้อมหูฟัง เครื่องฉายวิดีโอโปรเจกเตอร์ เป็นต้น

6) ภาพอนต์ร์



7) สั่งบันทึกเสียง



เช่น คอมพิวเตอร์พร้อมหูฟัง เครื่องบันทึกเสียง เป็นต้น

8) งานแพร่เสียงแพร่ภาพ



เช่น รายการโทรทัศน์ เป็นต้น

9) งานอื่นๆ ในแผนกวัฒนาคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ



เช่น การเพ้นท์ศิลปะบนร่างกาย เป็นต้น

ลิขสิทธิ์ กับ CREATIVE COMMONS ต่างกันอย่างไร ?



ลิขสิทธิ์

คือ สิทธิ์ที่มีเพียงผู้เดียวที่จะสามารถกระทำการทำต่อขึ้นงานที่มีลิขสิทธิ์



Creative Commons (ครีเอทีฟ คอมมอนส์)

เป็นองค์กรไม่แสวงหากำไร ที่สนับสนุนการแบ่งปันงานสร้างสรรค์และข้อมูล ตามแนวทางการใช้งาน และลิขสิทธิ์ในปัจจุบัน



Creative Commons ทำงานร่วมกับ “ลิขสิทธิ์”

โดยเสนอทางเลือก ให้เจ้าของลิขสิทธิ์แบ่งปันการใช้งานลิขสิทธิ์ให้คนอื่น ในรูปแบบของสัญญาอนุญาต ครีเอทีฟคอมมอนส์ (CC License) เป็นทางเลือกที่ยืดหยุ่นกว่าและตอบโจทย์ของเจ้าของลิขสิทธิ์แต่ละคนได้ตรงใจ



ประเภทของสัญญาอนุญาต CC License

1. Attribution (BY)



สัญลักษณ์เพื่อรับรองสิทธิเจ้าของลิขสิทธิ อนุญาตให้ผู้อื่นนำเนื้อหาหรือผลงานไปใช้ได้ คนที่จะนำไปใช้ต้องรับรู้ถึงผู้ถือลิขสิทธิเสมอ ต้องอ้างอิงด้วยว่ามาจากไหน

2. Share Alike (SA)



สัญลักษณ์เพื่อรับรองสิทธิเจ้าของลิขสิทธิ อนุญาตให้ผู้อื่นนำเนื้อหาหรือผลงานไปใช้ได้ คนที่จะนำไปใช้ต้องรับรู้ถึงผู้ถือลิขสิทธิเสมอ ต้องอ้างอิงด้วยว่ามาจากไหน

3. Non-Commercial (NC)



อนุญาตให้ทำซ้ำ แจกจ่าย นำไปแสดงและตัดแปลงงานได้ แต่ไม่อนุญาตให้นำไปใช้เชิงพาณิชย์ หรือทางการค้า

4. No Derivative Works (ND)



ห้ามมีการตัดแปลงงาน ทำซ้ำ แจกจ่าย นำไปแสดงได้เฉพาะงานตามต้นฉบับเดิมเท่านั้น

รูปแบบของการใช้ CC License

ที่มีให้เลือก 6 แบบตามขนาดของการแบ่งปันมากที่สุดถึงน้อยที่สุด

1. Attribution (BY)



เป็นสัญญาที่แบ่งปันมากที่สุด สามารถนำผลงานไปใช้ แสวงหาผลกำไรได้ แต่ต้องให้เครดิตเจ้าของผลงาน

2. Attribution - Share Alike (BY-SA)



สามารถนำผลงานไปใช้ แสวงหาผลกำไรได้ ต้องให้เครดิตเจ้าของผลงานและเผยแพร่เป็น CC License แบบเดียวกับต้นฉบับ

3. Attribution - No Derivative Works (BY-ND)



สามารถนำผลงานไปใช้ แสวงหาผลกำไรได้ ต้องให้เครดิตเจ้าของผลงาน แต่ห้ามดัดแปลงโดยเด็ดขาดต้องให้เครดิตเจ้าของผลงาน

4. Attribution (BY)



สามารถนำผลงานไปใช้ ต้องให้เครดิตเจ้าของผลงาน แต่ห้ามนำไปใช้
แสวงหาผลกำไร

5. Attribution - Non-Commercial - Share Alike (BY-NC-SA)



สามารถนำผลงานไปใช้ และแสวงหาผลกำไรได้ ต้องให้เครดิตเจ้าของผลงาน
และเผยแพร่เป็น CC License แบบเดียวกับต้นฉบับ

6. Attribution - No Derivative Works (BY-ND)



สามารถนำผลงานไปใช้ได้ ต้องให้เครดิตเจ้าของผลงาน แต่ห้ามนำไป
แก้ไข ดัดแปลง รวมถึงใช้แสวงหาผลกำไร

วิธีเช็คสิทธิ์สื่อ ก่อนนำมาใช้งาน

หลังจากเราได้ทราบแล้วว่า ผลงานที่ได้จากอินเทอร์เน็ตนั้นแบบไหน ใช้ได้หรือไม่ได้ เรามาดูสรุปเช็คลิสต์ลิขสิทธิ์การใช้สื่อ เพื่อความมั่นใจ และไม่ผิดกฎหมายกัน

ใช้ได้



- สร้างสรรค์รูปภาพรูปนี้ขึ้นมาเอง
- ใช้ภาพของผู้อื่นเพื่อรายงานข่าว การศึกษา หรืองานวิจัย
- ใช้ภาพของผู้อื่นที่มี Creative Commons เพื่อการค้าหรือกำไร ส่วนบุคคล โดยใช้ตามเงื่อนไขที่อนุญาต

ใช้ไม่ได้



- ภาพของผู้อื่นที่ไม่ได้รับอนุญาต จากแหล่งต้นฉบับ
- ใช้ภาพของผู้อื่นเพื่อการค้าหรือกำไรส่วนบุคคล โดยไม่จ่ายเงิน เพื่อใช้รูปภาพ

วิธีการใช้งานรูปที่ได้รับการอนุญาต

ง่าย ๆ จาก Google



ลองมาดูวิธีการง่าย ๆ ในการค้นหารูปบนอินเทอร์เน็ตที่ได้รับอนุญาตให้นำไปใช้งานได้ ดังนี้



กฎหมายกี่เกี่ยวข้อง



1) กรณีละเมิดลิขสิทธิ์โดยตรง

การกระทำอย่างใดอย่างหนึ่งแก่งานอันมีลิขสิทธิ์โดยไม่ได้รับอนุญาต ได้แก่ ทำซ้ำหรือดัดแปลง และนำออกเผยแพร่ต่อสาธารณะชน

มาตรา 69

ผู้ใดกระทำการละเมิดลิขสิทธิ์หรือลิขของนักแสดงตามมาตรา 271

มาตรา 282 มาตรา 293 มาตรา 304 หรือมาตรา 525

โทษ : ปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นการกระทำเพื่อการค้า ผู้กระทำต้องระวังโทษ จำคุกตั้งแต่หกเดือนถึงสี่ปี หรือปรับตั้งแต่หนึ่งแสนบาทถึงแปดแสนบาท หรือทั้งจำทั้งปรับ

2) กรณีละเมิดลิขสิทธิ์โดยอ้อม

การละเมิดโดยบุคคลโดยรู้อยู่แล้ว หรือมิเหตุอันควรรู้ว่างานได้ทำขึ้นโดยละเมิดลิขสิทธิ์ของผู้อื่น ซึ่งกระทำอย่างใดอย่างหนึ่งแก่งานนั้นเพื่อหากำไร

มาตรา 70 ผู้ใดกระทำการละเมิดลิขสิทธิตามมาตรา 316

โทษ : ปรับตั้งแต่หนึ่งหมื่นบาทถึง หนึ่งแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นการกระทำเพื่อการค้า ผู้กระทำต้องระวังโทษ จำคุกตั้งแต่สามเดือนถึงสองปี หรือปรับตั้งแต่ห้าหมื่นบาทถึงสี่แสนบาท หรือทั้งจำทั้งปรับ

การอ้างอิงแหล่งข้อมูล (Citation) ในงานวิจัย



การอ้างอิงแหล่งข้อมูล (Citation) ในงานวิจัย เป็นสิ่งสำคัญอย่างยิ่งที่แสดงถึงความน่าเชื่อถือ โปร่งใส และความถูกต้องของงานวิจัย ช่วยให้ผู้อ่านสามารถตรวจสอบข้อมูลย้อนหลัง เข้าถึงแหล่งข้อมูลต้นฉบับ และประเมินคุณภาพของงานวิจัยได้

รูปแบบการอ้างอิง

แต่ละรูปแบบมีรายละเอียด และวิธีการเขียนที่แตกต่างกัน ตัวอย่างรูปแบบที่นิยมใช้ ได้แก่

- APA (American Psychological Association) :
นิยมใช้ในสาขาสังคมศาสตร์ มนุษยศาสตร์ และบางสาขาวิทยาศาสตร์
- MLA (Modern Language Association) :
นิยมใช้ในสาขาวรรณกรรม ภาษาศาสตร์ และภาษาต่างประเทศ
- Chicago :
- นิยมใช้ในสาขาวิทยาศาสตร์ สังคมศาสตร์ และมนุษยศาสตร์
- Turabian :
- นิยมใช้ในสาขาวิทยาศาสตร์

ตัวอย่างการอ้างอิง

รูปแบบ APA :

Smith, J. (2023). The importance of citation in research. New York: Routledge.

รูปแบบ MLA :

Smith, John. The importance of citation in research. New York: Routledge, 2023.

รูปแบบ Chicago :

Smith, John. 2023. The importance of citation in research. New York: Routledge.

การอ้างอิงงานวิจัยออนไลน์ :

Smith, J. (2023, January 1). The importance of citation in research. Retrieved from <https://www.example.com/>

การอ้างอิงหนังสือ :

Smith, J. (2023). The importance of citation in research. New York: Routledge.

การอ้างอิงบทความในวารสาร :

Smith, J. (2023). The importance of citation in research. Journal of Research, 123(4), 567-578.

การอ้างอิงงานวิจัยภาษาไทย :

- หนังสือ : นามสกุล, ชื่อ. (ปีพิมพ์). ชื่อเรื่อง. สถานที่พิมพ์: สำนักพิมพ์.

ตัวอย่าง :

ศรีสุริโย, วรัญญา. (2566). ความสำคัญของ Citation ในงานวิจัย. กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

- บทความในวารสาร : นามสกุล, ชื่อ. (ปีพิมพ์). "ชื่อเรื่อง". ชื่อวารสาร, เล่มที่(หมายเลขอ), หน้า-หน้า.

ตัวอย่าง :

ศรีสุริโย, วรัญญา. (2566). "ความสำคัญของ Citation ในงานวิจัย". วารสารมหาวิทยาลัยธรรมศาสตร์, 55(2), 101-112.

- การอ้างอิงงานวิจัยจากฐานข้อมูลออนไลน์ :
นามสกุล, ชื่อ. (ปีพิมพ์). "ชื่อเรื่อง". ชื่อฐานข้อมูล, ชื่อแหล่งข้อมูล.
(DOI)

ตัวอย่าง :

ศรีสุริโย, วรัญญา. (2566). "ความสำคัญของ Citation ในงานวิจัย".
ฐานข้อมูล TCI, มหาวิทยาลัยธรรมศาสตร์. url เว็บไซต์ที่มา

การอ้างอิงงานประเภทอื่นๆ

- งานนำเสนอ :
นามสกุล, ชื่อ. (ปีพิมพ์). ชื่อเรื่อง. ประชุมวิชาการ ชื่อประชุม, สถาน
ที่จัดประชุม, วันที่จัดประชุม.
- รายงานการวิจัย :
นามสกุล, ชื่อ. (ปีพิมพ์). ชื่อเรื่อง. ชื่อหน่วยงาน.
- วิทยานิพนธ์ :
นามสกุล, ชื่อ. (ปีพิมพ์). ชื่อเรื่อง. วิทยานิพนธ์ (ระดับปริญญา), ชื่อ
มหาวิทยาลัย.

การอ้างอิงในเนื้อหา

มี 2 วิธีหลักในการอ้างอิงในเนื้อหา

1. การอ้างอิงแบบแทรกในเนื้อหา :

เขียนชื่อผู้แต่งและปีที่พิมพ์ในวงเล็บกลม (Smith, 2023)

2. การอ้างอิงแบบบรรณานุกรม :

เขียนรายการอ้างอิงทั้งหมดไว้ท้ายงานวิจัย

การจัดรูปแบบบรรณานุกรม

1. เรียงลำดับรายการอ้างอิงตามตัวอักษร
2. เว้นวรรค 2 ช่องสำหรับแต่ละบรรทัด
3. จัดย่อหน้าถัดไปให้เยี้ยงเข้า 0.5 นิ้ว

ตัวอย่างการจัดรูปแบบบรรณานุกรม

- Smith, J. (2023). The importance of citation in research. New York: Routledge.
- ศรีสุริโย, วรัญญา. (2566). ความสำคัญของ Citation ในงานวิจัย. กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

เครื่องมือช่วยอ้างอิง

มีเครื่องมือมากมายที่ช่วยในการอ้างอิง เช่น Zotero, Mendeley, EndNote ช่วยให้ผู้ใช้จัดการรายการอ้างอิง จัดรูปแบบการอ้างอิง และสร้างรายการอ้างอิงโดยอัตโนมัติ

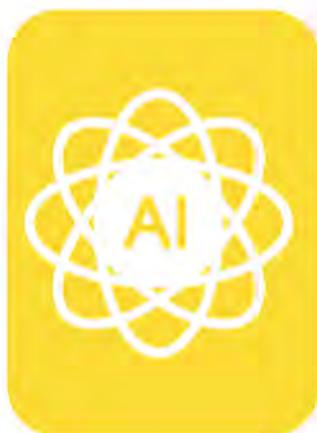
ข้อควรระวัง

- ตรวจสอบให้แน่ใจว่ารูปแบบการอ้างอิงถูกต้อง และสอดคล้องกันทั้งงานวิจัย
- อ้างอิงแหล่งที่มาทั้งหมดที่ใช้ในงานวิจัย
- หลีกเลี่ยงการลอกเลียนงานผู้อื่น





สืื่อเนื้อหาดิจิทัลหลายรูปลักษณ์
อยู่ที่ปักความต้องการซ่องทางขอบ
ดังนั้นผู้สร้างเนื้อหาต้องมีกรอบ
ทำรอบขอบถูกกฎหมายจริยธรรม
สร้างสรรค์งานควรเคารพลิขสิทธิ์
ใช้ความคิดไม่ลอกเลียนผลิตซ้ำ
ทุกงานเขียนงานสร้างวรรณกรรม
ให้เป็นธรรมกับเจ้าของต้องอ้างอิง



ถ้าคุณเรียนผ่านด้านนี้
คุณจะสามารถเพิ่มพูนทักษะ
ด้าน AI และใช้ประโยชน์
ได้อย่างสูงสุด

5.3

DATA & AI GOVERNANCE

วัตถุประสงค์

- ผู้เรียนสามารถอธิบายความหมาย ประเภท หลักการทำงานพื้นฐานของ AI ได้แก่ MACHINE LEARNING, NEURAL NETWORKS และ DEEP LEARNING ได้
- ผู้เรียนมีความรู้เกี่ยวกับ การใช้งาน AI ที่เกี่ยวข้องในชีวิตประจำวัน รวมถึงการใช้ประโยชน์จาก AI อุปกรณ์มีกรรมภัยบล็อก
- ผู้เรียนตระหนักรถึงผลกระทบ ความเสี่ยง และแนวปฏิบัติที่ควร และ ไม่ควรทำในการใช้ AI อุปกรณ์มีกรรมภัยบล็อก



ເກົ່າກັນ AI ເກມໂນໂລຍືເພື່ອວຸນາຄຕ



AI ย่อมาจาก Artificial Intelligence หากแปลตามราชบัณฑิตยสถาน แปลว่า “ปัญญาประดิษฐ์” อธิบายก็คือ ระบบประมวลผลของคอมพิวเตอร์ หรืออุปกรณ์อิเล็กทรอนิกส์ต่าง ๆ ที่มีการวิเคราะห์เชิงลึกคล้ายความฉลาดของมนุษย์ และทำให้เกิดผลลัพธ์ได้

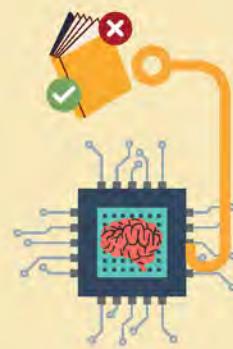
ປະເກດຂອງ AI

ແບ່ງອອກໄດ້ເປັນ 3 ປະເກດຫຼັກ ໄດ້ແກ່

1. Machine Learning (ML)

ເປັນສາขาຫຼັກຂອງ AI ທີ່ໃຫ້ຄົມພິວເຕອຮີມີຄວາມສາມາດໃນການເຮັດວຽກຂໍ້ມູນ ໂດຍໄມ້ຕ້ອງມີໂປຣແກຣມຍ່າງໜຶດເຈນ ທຳມະນາດໂດຍການວິເຄາະໜໍ້ຈຸດຂໍ້ມູນໃໝ່ເພື່ອຄັ້ນຫາຮຽບແບບ ແລະຄວາມສັນພັນນົດ

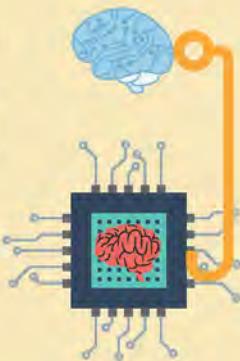
ປະໂຍ່ໜົນ : ປັບປຸງຄວາມແມ່ນຢໍາໃນການທຳນາຍຜລລັພ້ຈາກຂໍ້ມູນນາດໃໝ່



2. Neural Networks

มีการออกแบบโครงสร้าง ที่เลียนแบบเซลล์ประสาท ในสมองมนุษย์ ช่วยให้คอมพิวเตอร์สามารถจำแนก และตีความข้อมูลได้ซับซ้อน เช่น ภาพ เสียง เป็นต้น

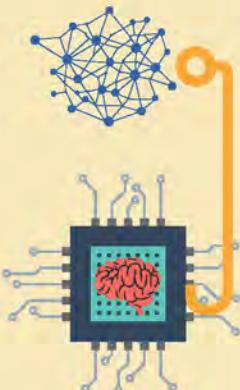
ประโยชน์ : ช่วยเพิ่มประสิทธิภาพในงานที่เกี่ยวกับ การจดจำและการประมวลผลภาพ



3. Deep Learning

เป็นส่วนขยายของ Neural Networks ที่ใช้ขั้นการ ประมวลผลหลายชั้นเพื่อวิเคราะห์ข้อมูล ช่วยให้ระบบ AI สามารถเรียนรู้ความสัมพันธ์ที่ซับซ้อนได้เอง

ประโยชน์: สามารถจำแนกและทำนายข้อมูลได้ อย่างแม่นยำสูง



โอกาสและความท้าทาย จาก AI



ยุคของ AI นำมาซึ่งการเปลี่ยนแปลงหลายอย่าง เนื่องจากประโยชน์ของ AI นั้นส่งผลต่อการดำเนินชีวิต เช่น

1 การแพทย์



มีส่วนช่วยหมอในการวินิจฉัยโรค หรือช่วยพัฒนาตัวยา

2 การศึกษา



มีส่วนในการพัฒนาหลักสูตร และช่วยให้การเรียนรู้ มีประสิทธิภาพ

3 ด้านธุรกิจ



ช่วยวิเคราะห์ข้อมูลและเพิ่มประสิทธิภาพในการทำงาน

4 การคมนาคม



มีการพัฒนาระบบติดตามรถคันขับ และระบบขนส่งอัจฉริยะ

ประเด็นของความท้าทาย ในการใช้ประโยชน์จาก AI

1. ความกังวลเรื่องความเป็นส่วนตัว และความปลอดภัยของข้อมูล

การเก็บรวบรวมและการวิเคราะห์ข้อมูลขนาดใหญ่ที่ AI ต้องการอาจเป็นความเสี่ยงต่อความเป็นส่วนตัวของบุคคล นอกจากนี้ ยังมีความเสี่ยงที่ข้อมูลนั้นอาจถูกใช้ในทางที่ผิดหรือถูกแฮกได้

2. การสูญเสียงาน

การอัตโนมัติที่เกิดจาก AI อาจนำไปสู่การสูญเสียงานในบางอาชีพทำให้เกิดความจำเป็นในการฝึกอบรมและการพัฒนาทักษะใหม่ ๆ สำหรับแรงงาน

3. ความเหลื่อมล้ำทางเทคโนโลยี

การเข้าถึง และการใช้ประโยชน์จาก AI อาจไม่เท่าเทียมกันในทุกสังคม ส่งผลให้เกิดความเหลื่อมล้ำทางเทคโนโลยีและเศรษฐกิจ

4. ความท้าทายทางจริยธรรม

การพัฒนาและการใช้ AI ต้องเผชิญกับคำถามทางจริยธรรม เช่น การควบคุมและการรับผิดชอบในกรณีที่ AI ตัดสินใจผิดพลาด การสร้าง AI ที่ไม่มีอคติและยุติธรรมเป็นความท้าทายที่สำคัญ

การใช้ AI ในชีวิตประจำวัน



AI ได้แทรกซึมเข้ามามีบทบาทในชีวิตประจำวันของเราในหลาย ๆ ด้าน ตัวอย่างที่พบเห็นได้ทั่วไป มีดังนี้

การสื่อสาร

- ผู้ช่วยเสมือนอัจฉริยะ เช่น Siri, Google Assistant และ Alexa ที่ใช้ AI ช่วยในการตอบคำถาม จัดการตารางเวลา ควบคุมอุปกรณ์ในบ้านอัจฉริยะ และอื่น ๆ
- การแปลภาษาแบบเรียลไทม์ เช่น Google Translate, Microsoft Translator
- การกรองข้อความขยะ (Spam)

การเดินทาง

- แอปพลิเคชันนำทาง เช่น Google Maps
- บริการรถเรียกผ่านแอปพลิเคชัน เช่น Grab, LINE MAN
- ระบบขนส่งอัตโนมัติ เช่น รถไฟฟ้าiron เป็นต้น

การซื้อ - ขายของออนไลน์

- ระบบแนะนำสินค้าอัจฉริยะบนเว็บไซต์ เช่น Amazon, Lazada, Shopee
- ซอฟต์แวร์สำหรับการตอบคำถามและให้บริการลูกค้า
- เทคโนโลยีการชำระเงินด้วยใบหน้า

ความบันเทิง

- แพลตฟอร์มสตรีมมิ่งวิดีโอ เช่น Netflix YouTube
- แอปพลิเคชันฟังเพลง เช่น Spotify Apple Music
- เกมที่ใช้ AI เช่น Dreamscape The Sims

สุขภาพและความเป็นอยู่ที่ดี

- อุปกรณ์ติดตามสุขภาพ เช่น Fitbit Apple Watch
- แอปพลิเคชันสำหรับติดตามการนอนหลับ
- ซอฟต์แวร์สำหรับให้คำปรึกษาด้านสุขภาพ

การศึกษา

- แพลตฟอร์มการเรียนรู้แบบออนไลน์ เช่น Khan Academy, Coursera
- ระบบติวเตอร์อัจฉริยะ
- เทคโนโลยีการตรวจสอบการลอกเลียนแบบ

ภาครัฐ

- การใช้ AI วิเคราะห์ข้อมูลเพื่อพัฒนาโยบายและบริการภาครัฐ
- การใช้ AI พัฒนาระบบเมืองอัจฉริยะ (Smart City)
- การใช้ AI ป้องกันอาชญากรรม



การใช้ประโยชน์จาก AI อย่างมีธรรมาภิบาล



ความหมายของ ธรรมาภิบาลใน AI

ธรรมาภิบาลใน AI หมายถึง การพัฒนาและการใช้งาน AI โดยคำนึงถึง หลักจริยธรรม ความโปร่งใส ความยุติธรรม และความรับผิดชอบ มีจุด มุ่งหมายเพื่อให้เทคโนโลยีนี้มีประโยชน์ต่อสังคมโดยรวมโดยไม่ส่งผลกระทบ ต่อบุคคลหรือกลุ่มคนใด

การใช้ AI อย่างมีธรรมาภิบาล สำหรับคนทั่วไป



- เลือกใช้ผลิตภัณฑ์และบริการที่โปร่งใสและมีจริยธรรม

ก่อนตัดสินใจใช้ผลิตภัณฑ์ หรือบริการ AI ได ๆ ควรศึกษาและ ทำความเข้าใจวิธีการทำงานของ AI เช่น แอปพลิเคชันที่เน้นนำ เนื้อหา โดยอาศัยระบบ Machine Learning หรือการเรียนรู้ของ ระบบ ความมีนโยบายความเป็นส่วนตัว และการใช้ที่ชัดเจน เป็นต้น

- ใช้งาน AI โดยคำนึงถึงความเป็นส่วนตัว ให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคล

เช่น การจำกัดการเข้าถึงข้อมูลส่วนตัวบนอุปกรณ์สมาร์ตโฮม หรือการปรับการตั้งค่าความเป็นส่วนตัวบนโซเชียลมีเดียที่ใช้ AI ใน การแนะนำเนื้อหา

- สนับสนุนและใช้ผลิตภัณฑ์ที่มีการพัฒนาอย่างยั่งยืน
สนับสนุนบริษัทและองค์กรที่ใช้ AI เพื่อการพัฒนาที่ยั่งยืน

เช่น การใช้ AI ในการปรับปรุงระบบพลังงาน การจัดการขยะ หรือ การเกษตรที่มีประสิทธิภาพ

- มีส่วนร่วมในการสร้างความตระหนักรู้ และการศึกษาเกี่ยวกับ AI ให้โอกาสในการศึกษาและส่งเสริมความตระหนักรู้ เกี่ยวกับ AI และ จริยธรรมในการใช้งาน เพื่อให้สังคมมีความเข้าใจ และสามารถใช้ เทคโนโลยีได้อย่างรับผิดชอบ

- มีส่วนร่วมในการตั้งคำถามและวิพากษ์วิจารณ์

เมื่อpub เห็นการใช้งาน AI ที่อาจนำไปสู่ความไม่เป็นธรรมหรือละเมิดจริยธรรม มีส่วนร่วมในการตั้งคำถามและวิพากษ์วิจารณ์ผ่านช่องทางต่าง ๆ เช่น โซเชียลมีเดีย หรือการรณรงค์



ความเสี่ยงจาก การใช้เทคโนโลยี AI

ในขณะที่ปัญญาประดิษฐ์ (AI) เริ่มมีบทบาทสำคัญในหลายด้านของชีวิต และการทำงาน แต่ในทางกลับกันก็นำมาซึ่งความเสี่ยง และความท้าทาย ที่ไม่គุรมองข้าม

ความเสี่ยงจากการใช้เทคโนโลยี AI

- ความเสี่ยงต่อความเป็นส่วนตัวและข้อมูล

หนึ่งในความเสี่ยงหลักของ AI คือ การละเมิดความเป็นส่วนตัว ระบบ AI ที่วิเคราะห์ข้อมูลส่วนบุคคลอาจเปิดโอกาสให้ข้อมูลนั้นถูกใช้งานอย่างไม่เหมาะสมหรือรั่วไหล ซึ่งสามารถนำไปสู่การละเมิดสิทธิส่วนบุคคลและความเสี่ยงด้านความปลอดภัยข้อมูล

- ความเสี่ยงต่อการเกิดอคติและการตัดสินใจที่ไม่ยุติธรรม AI

หาก AI ได้รับข้อมูลที่มาอคติมากเกินไป สามารถสร้างผลลัพธ์ที่ไม่ยุติธรรม โดยเฉพาะในการตัดสินใจที่เกี่ยวข้องกับการจ้างงาน การให้สินเชื่อ หรือการพิจารณาคดีทางกฎหมาย ซึ่งอาจนำไปสู่การเลือกปฏิบัติและความไม่เท่าเทียม

• ความเสี่ยงต่อการสูญเสียงาน

การอัดโน้มติที่ขับเคลื่อนโดย AI สามารถทำหน้าที่แทนมนุษย์หลายงาน นำไปสู่ความกังวลเรื่องการสูญเสียงานและความท้าทายในการทำงานใหม่สำหรับแรงงานในอุตสาหกรรมที่ได้รับผลกระทบ

• ความเสี่ยงต่อความปลอดภัย AI

มีความสามารถในการปรับปรุงระบบความปลอดภัย ในขณะเดียวกัน ก็สร้างความเสี่ยงใหม่ ๆ เช่น การใช้ AI ใน การพัฒนามัลแวร์ หรือ การโจมตีทางไซเบอร์ที่ซับซ้อนขึ้น นอกจากนี้ AI ที่ควบคุมอาวุธ หรือระบบสำคัญ อาจนำไปสู่ความเสี่ยง ที่ไม่สามารถคาดการณ์ได้ หากถูกใช้งานอย่างไม่เหมาะสม

• ความเสี่ยงต่อการควบคุมที่ลดลง

การพัฒนา AI ที่มีความสามารถสูงสุดอาจนำไปสู่สถานการณ์ที่มนุษย์ ไม่สามารถควบคุมหรือทำความเข้าใจการตัดสินใจของระบบ AI ได้ เราต้องการกลไกในการตรวจสอบและควบคุม AI เพื่อให้แน่ใจว่ามันทำงานได้ตามวัตถุประสงค์และไม่สร้างความเสี่ยงที่ไม่คาดคิด



TIP

รวมรูปแบบของ AI ที่มิจฉาชีพนำไปใช้

สำหรับตรวจสอบสุนกกลาง (CIB) ได้รวบรวมรูปแบบของ AI ที่มิจฉาชีพนำไปใช้ ดังนี้

- Voice Cloning



หรือ การใช้ AI ปลอมเสียง โดยจะเป็นการใช้ AI เลียนแบบเสียงของบุคคลให้มีความคล้ายคลึงกับบุคคล เพื่อใช้ในการหลอกเหยื่อให้คิดว่าได้คุยกับคน ๆ นั้นจริง ๆ ก่อนที่จะหลอกให้โอนเงินหรือทำอะไรอย่างอื่นต่อไป

- Deepfake



หรือการใช้ AI ปลอมแปลงใบหน้าให้มีความคล้ายคลึงกับบุคคลต่าง ๆ เพื่อหลอกเชื่อว่าคน ๆ นั้น ได้ทำแบบนั้นจริงหรือปลอมเป็นคนใกล้ตัวเพื่อหลอกเหยื่อ ให้หลงเชื่อ

**TIP**

- Fake Business หรือ การใช้ Generative AI ต่าง ๆ



ในการสร้างบทความ หรือสคริปต์วิดีโอเพื่อให้ดูเป็นมืออาชีพด้านต่าง ๆ เพื่อหลอกเหยื่อให้มาร่วมลงทุน หรือใช้ร่วมกันทั้ง 2 ข้อเพื่อความแนบเนียน

วิธีป้องกันเบื้องต้น

- สังเกตจังหวะการเว้นวรรคคำพูด น้ำเสียง เสียงวรรณยุกต์ ว่ามีจังหวะเว้นวรรคตอนแปลกรๆ หรือไม่ มีน้ำเสียงราบรื่นเกินไป ใหม มีจังหวะหายใจใหม หรือออกเสียงวรรณยุกต์สูงต่ำ ผิดเพี้ยน หรือไม่
- หากเป็นคลิปวิดีโอ ที่ต้องสงสัย ให้สังเกตการขยายบาก ของคนในคลิปว่าเป็นธรรมชาติหรือไม่ มีสัดส่วนผิดเพี้ยน หรือสีผิด ดำ ๆ ด่าง ๆ หรือไม่ หรือมีการกระพริบตาถี่หรือน้อยเกินไปหรือไม่



TIP

- หากเป็นการวิดีโอกอล แล้วคนที่โทรมาดูແปลกไปจากเดิม ให้ลองถามคำถามเรื่องส่วนตัวที่มีแต่คนในครอบครัวเท่านั้นที่รู้ดูก่อน หากปลายทางตอบไม่ได้ ให้สันนิษฐานไว้ก่อนว่าเป็นมิจฉาชีพ
- ก่อนโอนเงิน หรือ ทำธุรกรรมใด ๆ ให้สังเกตชื่อบัญชี ก่อนโอน ทุกครั้ง ว่าตรงกันกับบัญชีที่เราจะโอนหรือไม่ หากโอนบอกให้จ่ายค่าสินค้า ให้ก่อน ให้ลองปฏิเสธก่อน ห้ามโอนไปที่ร้านโดยตรง เพราะอาจ เป็นการโอนเข้าบัญชีม้า หรือบัญชีมิจฉาชีพได้
- สุดท้ายมีสติเสมอ หรือคิดให้รอบคอบก่อนที่จะตัดสินใจลงเชื้อ หรือโอนเงิน

ขอบคุณข้อมูล : กองบัญชาการตำรวจนครบาล

Do / Don't ในการใช้ AI



คำแนะนำ เกี่ยวกับ Do / Don't ในการใช้ AI สำหรับคนทั่วไป เพื่อให้ การใช้งาน AI เป็นไปอย่างมีความรับผิดชอบ และปลอดภัยมากยิ่งขึ้น

Do (ควรทำ)



- ศึกษาและเข้าใจ AI :

ใช้เวลาศึกษาเกี่ยวกับ AI และวิธีการทำงาน ของมัน เข้าใจถึงข้อจำกัดและศักยภาพของ เทคโนโลยี

- ปกป้องข้อมูลส่วนบุคคล :

ใช้การตั้งค่าความเป็นส่วนตัวและระดับระวัง ใน การให้ข้อมูลส่วนบุคคลกับแอปพลิเคชัน หรือบริการที่ใช้ AI

- ใช้ AI เพื่อเพิ่มประสิทธิภาพ :

ใช้ AI เพื่อเพิ่มประสิทธิภาพในการทำงาน และชีวิตประจำวัน เช่น การใช้ AI ในการ จัดการกับอีเมลหรือการจัดตารางงาน

- ใช้ AI อย่างมีจริยธรรม :

สนับสนุนและใช้ผลิตภัณฑ์ AI ที่ถูกพัฒนา อย่างมีจริยธรรมและโปร่งใส

Don't

(ไม่ควรทำ)



- อย่าละเลยความเป็นส่วนตัว :

อย่าละเลยการตั้งค่าความเป็นส่วนตัวหรือให้ข้อมูลส่วนบุคคลกับแอปพลิเคชันหรือบริการโดยไม่ได้ตรวจสอบเงื่อนไขและนโยบายความเป็นส่วนตัว

- อย่าเชื่อมั่น AI อย่างสมบูรณ์ :

อย่าเชื่อมั่นในผลลัพธ์จาก AI อย่างไม่มีข้อสงสัย ควรมีการตรวจสอบและวิเคราะห์ข้อมูลด้วยตนเอง

- อย่าใช้ AI โดยไม่คำนึงถึงผลกระทบ :

อย่าใช้ AI ในวิธีที่อาจนำไปสู่ผลกระทบทางลบต่อผู้อื่นหรือสังคม โดยไม่ได้พิจารณาถึงความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้น

- อย่าลืมการพัฒนาทักษะของตนเอง :

อย่าพึ่งพา AI อย่างเดียวในการทำงาน หรือการตัดสินใจ ควรพัฒนาทักษะและการเรียนรู้อย่างต่อเนื่องเพื่อทำงานร่วมกับ AI ได้อย่างมีประสิทธิภาพ

**TIP**

การเขียน Prompt ทักษะใหม่กี่ควรรู้ในการใช้ AI อย่างมีประสิทธิภาพ



Prompt คืออะไร ?

คือ คำสั่ง หรือชุดคำสั่งที่มนุษย์ป้อนให้กับ AI เพื่อกระตุ้นให้ AI สร้างผลลัพธ์ที่ต้องการ ไม่ว่าจะเป็น การสร้างข้อความ รูปภาพ โคด หรือการกระทำอื่น ๆ Prompt เปรียบเสมือนสะพานเชื่อมระหว่าง ความคิดของมนุษย์กับความสามารถของ AI ใน การประมวลผล และสร้างสรรค์

ความสำคัญของ Prompt

Prompt มีความสำคัญอย่างยิ่งในการใช้งาน AI เพราะเป็นตัวกำหนดทิศทาง และคุณภาพของผลลัพธ์ที่ AI สร้างขึ้น Prompt ที่ดีจะช่วยให้ AI เข้าใจความต้องการของผู้ใช้ได้อย่างถูกต้อง และแม่นยำ ส่งผลให้ผลลัพธ์ที่ได้มีประสิทธิภาพ และตรงตามความคาดหวัง

**TIP****Prompt กับประโยชน์ทางธุรกิจ**

ในการทำธุรกิจ การเลือกใช้ Prompt ที่ดีสามารถช่วยให้เราได้รับข้อมูลที่มีคุณค่า และมีประโยชน์จาก AI ช่วยในการวิเคราะห์ข้อมูลรวมถึงการตัดสินใจ หรือแม้แต่ในการสื่อสารกับลูกค้าทางธุรกิจด้วย

Prompt กับประโยชน์ในการบริหารจัดการ

นอกจากนี้ Prompt ยังสามารถใช้ในการสร้างรายงาน การวิเคราะห์ผลการทำงาน หรือแม้แต่เป็นตัวช่วยในการสร้างแผนการตลาด ช่วยให้การทำงานของเราและทีมงานเป็นเรื่องที่ง่าย และรวดเร็วยิ่งขึ้น

Prompt กับประโยชน์ในการศึกษา

สำหรับนักเรียนนักศึกษา หรือผู้ที่สนใจใน AI การใช้ Prompt ที่ดีสามารถช่วยให้สามารถนำ AI ไปใช้ค้นหาข้อมูลในการเรียนรู้ และทำความเข้าใจบทเรียนได้ง่ายขึ้น รวมถึง ช่วยในการวิเคราะห์ข้อมูลเพื่อทำรายงานหรือสรุปบททวนบทเรียน



TIP

8 เทคนิคการเขียน Prompt ยังไง ให้ AI เข้าใจเรามากที่สุด



การเขียน Prompt ที่มีประสิทธิภาพ คือการสื่อสารกับ AI อย่างชัดเจนและตรงประเด็น เพื่อให้ AI สามารถเข้าใจ และตอบสนองต่อความต้องการได้อย่างถูกต้อง โดยได้มีการรวบรวมเทคนิคการเขียน Prompt ดังนี้

1. กำหนดบทบาท

ก่อนเริ่มต้นบทสนทนา เราต้องคิดก่อน ว่าต้องการให้ AI ประมวลผล และทำอะไรให้กับเรา แล้วเราจะจึงกำหนดบทบาทตามหน้าที่ที่สามารถทำได้ ในคำสั่งนั้น ๆ โดยมีคำสั่งสั้น ๆ อย่างเช่น

“As a ...” หรือ “ในฐานะ ...”

ยกตัวอย่าง : “As a content creator, ...” หรือ “ในฐานะ Content Creator ...” เป็นต้น

 TIP

2. กำหนดเป้าหมายที่ชัดเจน และเฉพาะเจาะจง

เมื่อรู้แล้วว่าต้องการให้ AI เล่นเป็นบทบาทอะไร ต่อมาเราจึงเขียนคำสั่งต่อจากการกำหนดบทบาทให้ AI รู้ว่า เราต้องการให้คิด และสร้างอะไรมาก่อน ให้กับเรา เช่น ให้สร้างเนื้อหา แปลภาษา เขียนโค้ด หรือตอบคำถาม

ยกตัวอย่าง : “As a content creator, write a content to promote products, ...” หรือ “ในฐานะ Content Creator เขียนคอนเทนต์เพื่อโปรโมทสินค้าให้หน่อย ...” เป็นต้น

3. กำหนดรายละเอียด หรือขั้นตอนต่าง ๆ

ในการสร้างสิ่งใดสิ่งหนึ่งขึ้นมาให้เป็นไปตามที่เราต้องการ จำเป็นต้องเขียนคำสั่ง เพื่อบอกถึงรายละเอียด หรือลำดับขั้นตอนอย่างชัดเจนที่ต้องการให้ AI รับรู้และแสดงผลออกมา เพื่อให้ผลลัพธ์ออกมาถูกต้อง และตรงใจเรามากที่สุด

ยกตัวอย่าง : ในการสร้างสิ่งใดสิ่งหนึ่งขึ้นมาให้เป็นไปตามที่เราต้องการ จำเป็นต้องเขียนคำสั่ง เพื่อบอกถึงรายละเอียด หรือลำดับขั้นตอนอย่างชัดเจนที่ต้องการให้ AI รับรู้และแสดงผลออกมา เพื่อให้ผลลัพธ์ออกมาถูกต้อง และตรงใจเรามากที่สุด



4. ใช้ภาษาที่กระชับ ชัดเจน และเป็นธรรมชาติ

หลีกเลี่ยงการใช้คำศัพท์ที่กำกัง หรือประโยคที่ซับซ้อนเกินไป ใช้ภาษาที่เป็นธรรมชาติ เมื่อถูกกับที่ใช้สื่อสารกับคนทั่วไป

5. ระบุรูปแบบผลลัพธ์

เป็นการบอก AI ว่าเราต้องการให้ผลลัพธ์ของข้อความที่ได้ออกมาเป็นแนวไหน แสดงความรู้สึกอย่างไรออกมาจากตัวหนังสือ หรืออยากให้ผู้อ่านรู้สึกอย่างไร เช่น ต้องการให้ออกมาในรูปแบบทางการ เหมาะสมกับการประชุม หรือต้องการให้ออกมาในรูปแบบสนุกสนาน สามารถ Entertain ผู้อ่านได้ เป็นต้น

6. จำกัด Scope ของข้อความ

การจำกัด Scope ของงานให้เป็นไปตามที่เราต้องการ ทั้งการจำกัดจำนวนคำในข้อความ และการระบุเป้าหมายหลักที่ต้องการจะนำไปเผยแพร่ เช่น ต้องการจำกัดให้ผลลัพธ์ออกมาอยู่ภายใน 2,000 คำ และเน้นว่าให้เหมาะสมกับการทำการทำตลาดแบบออนไลน์ เป็นต้น

**TIP****7. ยกตัวอย่าง เพื่อเป็นแนวทาง**

หากเป็นไปได้ ให้ยกตัวอย่างสิ่งที่ต้องการ เพื่อให้ AI เข้าใจรูปแบบที่ต้องการได้ง่ายขึ้น ตัวอย่างสามารถเป็นข้อความ รูปภาพ หรือโค้ด ก็ได้

8. ทดลอง ปรับปรุง และทำซ้ำ

การเขียน Prompt ที่ดีต้องอาศัยการทดลอง และปรับปรุงอย่างต่อเนื่อง โดยลองใช้ Prompt ที่เขียน จากนั้นดูผลลัพธ์ หากยังไม่ตรงใจ ให้ลองปรับปรุงแก้ไข Prompt หรือให้รายละเอียดเพิ่มเติม

ตัวอย่างการเขียน Prompt ที่ดี

Prompt ที่ไม่ดี เช่น เขียนบทความเกี่ยวกับสุขภาพ

Prompt ที่ดี เขียนบทความเกี่ยวกับประโยชน์ของการออกกำลังกาย สำหรับผู้สูงอายุ ความยาวประมาณ 500 คำ ใช้ภาษาที่เข้าใจง่าย และเป็นกันเอง เน้นให้ข้อมูลที่เป็นประโยชน์และน่าเชื่อถือ

อนาคตของ AI



AI จะแทนที่งานแบบมุษย์หรือไม่ ?

AI จะแทนที่งานบางประเภท แต่ก็จะสร้างงานใหม่ ๆ ขึ้นมา ทักษะสำคัญ สำหรับอนาคต คือ ทักษะดิจิทัล ทักษะการคิดวิเคราะห์ และทักษะการสื่อสาร

เราจะเรียนรู้เกี่ยวกับ AI ได้อย่างไร ?

การเรียนรู้เกี่ยวกับ AI สามารถทำได้ผ่านหลายช่องทาง ทั้งออนไลน์และออฟไลน์ ตามความสนใจและระดับความรู้ของแต่ละบุคคล

แหล่งเรียนรู้เกี่ยวกับ AI ที่มีประโยชน์และหลากหลาย



1) บล็อกและเว็บไซต์

- Towards Data Science : เป็นชุมชนบน Medium ที่มีบทความจำนวนมากเกี่ยวกับ AI, Machine Learning และ Data Science
- AI Google Blog : บล็อกอย่างเป็นทางการของ Google เกี่ยวกับ AI ที่มีข้อมูลการวิจัยและโปรเจกต์ล่าสุด

- ศูนย์ AIGC by ETDA (ศูนย์ธรรมาภิบาลปัญญาประดิษฐ์ : AI Governance Clinic) : ศูนย์กลางให้ความรู้และสนับสนุนการใช้ AI อย่างมีธรรมาภิบาล จาก ETDA :
<https://www.etda.or.th/th/Our-Service/AIGC/index.aspx>

2) หลักสูตรออนไลน์

- Coursera : มีหลักสูตรเกี่ยวกับ AI มากมายจากมหาวิทยาลัยชั้นนำทั่วโลก เช่น "Machine Learning" โดย Andrew Ng จาก Stanford University
- edX : แพลตฟอร์มนี้เสนอหลักสูตรจากสถาบันชั้นนำ เช่น "Introduction to Artificial Intelligence (AI)" จาก Microsoft
- Udacity : มีโปรแกรม Nanodegree ในหัวข้อ AI และ Machine Learning ที่เน้นการเรียนรู้โดยการปฏิบัติ

3) แหล่งเรียนรู้แบบอوفไลน์

- มหาวิทยาลัย : หลายมหาวิทยาลัยในประเทศไทยมีหลักสูตรเกี่ยวกับ AI
- งานสัมมนาและเวิร์กช้อป : มีการจัดงานสัมมนาและเวิร์กช้อปเกี่ยวกับ AI อยู่บ่อยครั้ง

- หนังสือ : ห้องสมุดมีหนังสือเกี่ยวกับ AI เช่น
- "Artificial Intelligence : A Modern Approach" โดย Stuart Russell และ Peter Norvig : เป็นหนังสือที่อ้างอิงกันอย่างกว้างขวางในด้าน AI
- "Deep Learning" โดย Ian Goodfellow, Yoshua Bengio, และ Aaron Courville : เน้นเรื่องการเรียนรู้เชิงลึก (Deep Learning) ซึ่งเป็นสาขาหนึ่งของ AI

4) วิดีโอและเนื้อหาวิดีโอ

- YouTube : มีช่องที่เน้นเกี่ยวกับ AI เช่น Siraj Raval, Lex Fridman ที่เสนอทั้งบทบาทพูดคุยและการสอนเกี่ยวกับ AI
- Podcasting : มี Podcasting มากมายที่พูดคุยเกี่ยวกับ AI
- TED Talks : มีการบรรยายหลายโดยผู้เชี่ยวชาญในด้าน AI ที่สามารถให้มุมมองใหม่ ๆ เกี่ยวกับเทคโนโลยีนี้

5) ฟอรั่มและชุมชนออนไลน์

- Reddit : มี subreddit เช่น r/MachineLearning ที่เป็นที่รวมของชุมชนผู้สนใจเกี่ยวกับ Machine Learning และ AI
- GitHub : เป็นแหล่งที่ดีในการค้นหาโปรเจกต์และค้นคว้าโค้ดเกี่ยวกับ AI ที่เปิดให้สาธารณะเข้าถึง

อนาคตของ AI คืออะไร ?

**อนาคตของ AI
มีแนวโน้มที่จะเติบโต
และมีบทบาทมากขึ้นในสังคม**



การพัฒนา AI ที่มีธรรมาภิบาล การควบคุมและการกำกับดูแลที่เหมาะสมจะเป็นสิ่งสำคัญ ในการใช้ประโยชน์จากเทคโนโลยีนี้ให้ได้มากที่สุด ในขณะเดียวกัน ก็ต้องระมัดระวังความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

การใช้ AI ย่อมตามมาด้วยความรับผิดชอบ การตระหนักรู้และความเข้าใจ เพื่อให้สุดท้ายเราสามารถนำเทคโนโลยีนี้ไปใช้เพื่ออนาคตที่ดี ได้อย่างแท้จริง





บทส่งท้าย ให้ชวนคิด พิศ “เอไอ”
 เท่าทันไว้ ใช้ได้เลิศ ก่อเกิดผล
 ช่วยเขียนวด Gen-สร้าง-เสริม เพิ่มพูนลั่น
 พัฒนา ฝึกฝน Prompt กล่อมกลไก
 แต่อย่าเพิ่ง รับทุกเมื่อ เชื่อทุกสิ่ง
 ยิ่งดูจริง ยิ่งต้องตรวจ เข้มงวดไว้
 ลับทักษะ ตระหนักรู้ คู่เอไอ
 ใช้ปลอดภัย รับผิดชอบ รอบคอบเบย

รู้เท่ากันดิจิทัล
กักษะจำเป็น
เพื่อชีวิตออนไลน์

แหล่งข้อมูลดิจิทัล

รูปแบบของ
แหล่งข้อมูลดิจิทัล

เกณฑ์แบ่งประเภท
แหล่งข้อมูลดิจิทัล

ประโยชน์ของ
แหล่งข้อมูลดิจิทัล

ตัวอย่าง
แหล่งข้อมูลดิจิทัล

การเลือกใช้ร้าน
แหล่งข้อมูลดิจิทัล

หลักการเข้าถึง
แหล่งข้อมูลดิจิทัล

แนวทางการรับชมสื่อ
อย่างรู้เท่ากัน

ควรหันกลับ
ธรรมชาติของสื่อ

ตรวจสอบ
แหล่งที่มาของข้อมูล

ใช้วิจารณญาณ
ในการรับชมสื่อ

ไม่ควรรับชมสื่อ
จากแหล่งเดียว

มีส่วนร่วมในการ
แลกเปลี่ยนข้อมูล

5.1

Media & Information

ธรรมชาติของสื่อ

ประเภทของ
ธรรมชาติของสื่อ

สื่อ คือ สิ่งที่ถูก
สร้างขึ้นมาจากมนุษย์

สื่อส่วนใหญ่ที่มี
เป้าหมายธุรกิจ

สื่อสร้างค่านิยม
และอุดมคติ

สื่อทำให้เกิดผล
ทางการเมืองและสังคม

สื่อมีอุดมคติ
และข้อจำกัดเฉพาะตัว

ด้านที่
5

การประเมินคุณภาพ
และความถูกเชื่อถือ
ของข้อมูลจากสื่อดิจิทัล

ปัจจัยที่ใช้พิจารณา
การประเมินคุณภาพ /
ความถูกเชื่อถือของข้อมูล

รู้เท่าทัน Fake News

ประเภทของข้อมูลเท็จ

การตรวจสอบเบื้องต้น

สาเหตุที่มาของข้อมูลเท็จ

ศิลปะแห่งการจัดการ
ข้อมูลจากสื่อดิจิทัล
ด้วยตนเอง

แนวทางการจัดการข้อมูล

ผลจากการแบ่งปัน
เนื้หาที่ไม่เหมาะสม

ข้อมูลใดบ้าง ที่ทำบันโภคดิจิทัล
แล้วขัดต่อกฎหมาย/จริยธรรม

การกระทำ /
พฤติกรรม

ผลกระทบ
ทางกฎหมาย

ผลกระทบ
ทางจริยธรรม

5.2 Digital Content Creation

สื่อและเนื้อหาดิจิทัล
มีรูปแบบที่หลากหลาย

สื่อและเนื้อหาดิจิทัล
มีรูปแบบที่หลากหลาย

ขั้นอยู่กับวัตถุประสงค์
รูปแบบการนำเสนอ
และช่องทางการเผยแพร่

ลิขสิทธิ์ กับ
CREATIVE COMMONS

การสร้างเนื้อหาดิจิทัล
ให้ดึงดูด
และเกิดการจดจำ

แนวทาง
การสร้างเนื้อหา

หลักการสร้างเนื้อหา
ให้ดึงดูดกฎหมาย
และจริยธรรม

กรณีศึกษา

ตัวอย่างเครื่องมือ
และแหล่งข้อมูล

การอ้างอิงแหล่งข้อมูล
ในงานวิจัย

รูปแบบการใช้
CC License

ประเภทของงานมีลิขสิทธิ์

รูปแบบการอ้างอิง

วิธีเข้าถึงสิทธิ์สื่อ
ก่อนนำมาใช้งาน

ลิขสิทธิ์
กับ CREATIVE COMMONS
ต่างกันอย่างไร ?

การอ้างอิงในเนื้อหา

วิธีการใช้งานรูปที่ได้รับ
อนุญาต จาก Google

ประเภทของสัญญาอนุญาต
CC License

การจัดรูปแบบบรรณานุกรม

กฎหมายที่เกี่ยวข้อง

เครื่องมือช่วยอ้างอิง

ตัวอย่างการจัด
รูปแบบบรรณานุกรม

5.3 Data & AI Governance

ทำาทัน AI

ประเภทของ AI

ความเสี่ยงจาก
การใช้เทคโนโลยี AI

ความเสี่ยงจาก
การใช้เทคโนโลยี AI

รวมรูปแบบของ AI
ที่มีจะมาเป็นไปใช้

วิธีป้องกันเบื้องต้น

โอกาส
และความท้าทาย
จาก AI

ประเภทของความท้าทาย
ในการใช้ประโยชน์จาก AI

Do / Don't
ในการใช้ AI

Do (ควรทำ)

Don't (ไม่ควรทำ)

การใช้ประโยชน์
จาก AI

ความหมายของ
ธรรมภัยภายใน AI

การใช้ AI
อย่างมีธรรมาภิบาล

แนวทาง
การสร้างเนื้อหา

การเขียน
Prompt

อนาคตของ AI

แหล่งเรียนรู้เกี่ยวกับ AI

แนวโน้มที่จะเติบโตของ AI

เอกสารอ้างอิง

กระทรวงยุติธรรม. (2564). กฎหมายน่ารู้ ตอนที่ 284 : หยุดการ Cyberbullying โทษจำคุก 1 ปี ปรับ 2 หมื่นบาท. สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://www.moj.go.th/view/56312>

คณะจิตวิทยา จุฬาลงกรณ์มหาวิทยาลัย. (2566). การข่มเหงรังแกทางโลกไซเบอร์ Cyberbullying. สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://www.psy.chula.ac.th/en/featurearticles/cyberbullying/>

จับแล้วหนุ่มหลอกเด็ก 17 ถ่ายคลิปโป๊แบล็กเมล์ดิจิทัล. (2565, มีนาคม 18). สำนักข่าวไทย อสมท. <https://tna.mcot.net/region-905729>

ดวงรัตน์ วงศ์เกลี้ดแก้ว. (2564). 6 สัญญาณ ที่บ่งบอกว่าลูกกำลังเสพติดสือออนไลน์. สืบค้นเมื่อ 5 มิถุนายน 2567, จาก <https://cityly.me/X9ePm>

เตือนภัยคนโสด ระวังถูกหลอกให้รักแล้วโอนเงิน. (2567, กุมภาพันธ์ 15). Thairath Money. https://www.thairath.co.th/money/economics/thailand_econ/2763359

ธนาคารที่เอ็มบีรนชาต (ttb). (2567). KYC คืออะไร. สืบค้นเมื่อ 4 มิถุนายน 2567, จาก <https://www.ttbbank.com/th/corporate/corp-digital-banking-and-other-services/other-service-crop/kyc-cdd>

ธนาคารแห่งประเทศไทย. (2562, 2 กันยายน). ประกาศธนาคารแห่งประเทศไทย เรื่อง หลักเกณฑ์การรับฝากเงินหรือการรับเงินจากประชาชนของสถาบันการเงินเฉพาะกิจ.

โรมีส กวадามูซ, วรรลัญช์ วรชวรวัลย์ และ ณัฐรัชต สามเมาะ. (2566).

ภูมิคุ้มกันในโลกดิจิทัล (Digital Resilience) ทักษะที่เด็กและเยาวชนไทยยุคใหม่ต้องมี. สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://citly.me/5PbXx>

บริษัท ดิตโต (ประเทศไทย) จำกัด (มหาชน). (2566). ระบบยืนยันตัวตนแบบ E-KYC และ KYC คืออะไร และต่างกันอย่างไร. สืบค้นเมื่อ 4 มิถุนายน 2567, จาก <https://www.dittothailand.com/dittonews/gov-what-is-e-kyc/>

บริษัท เสนาดีเวลลอปเม้นท์ จำกัด (มหาชน). (2565). กฎเบรกตา 20-20-20. สืบค้นเมื่อ 5 มิถุนายน 2567, จาก <https://www.sena.co.th/articles/break-eye>

ปริญญา หอมเอนก. (2566). ทำความรู้จักกับ Information Disorder “ความผิดปกติของข้อมูลข่าวสาร” สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://citly.me/BrKWD>

พีรพล อนุตรโสตถี และ เจรจา ศala Wong. (2564). คู่มือภาคปฏิบัติ นักตรวจสอบข้อเท็จจริง (FACT-CHECK in ACTION). พิมพ์ครั้งที่ 2. กรุงเทพฯ: คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

ภูริชัย อรัญญู. (2567). ‘No.1 คือการสื่อสาร’ ทักษะที่น่ายั่งต้องการมากที่สุด และ Soft Skill อะไรบ้างที่มีลงในปี 2024. สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://www.blockdit.com/posts/66544213f864a30fba993157>

ศิริกร เอื้อไฟจิตร. (2562, กรกฎาคม 8). BBC NEWS ไทย. <https://www.bbc.com/thai/thailand-48902824>

สรานนท์ อินทนนท์. (2563). การบริหารจัดการเวลาบนโลกดิจิทัล (Screen Time Management). พิมพ์ครั้งที่ 2. กรุงเทพฯ: มูลนิธิส่งเสริมสื่อเด็กและเยาวชน (สสย.).

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2566, 13 มีนาคม).

ประกาศข้อเสนอแนะมาตรฐานฯ ว่าด้วยการพิสูจน์และยืนยันตัวตน ทางดิจิทัล เวอร์ชัน 3.0 จำนวน 3 ฉบับ.

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2555). **Fake News** ลงให้เชื่อ หลอกให้แชร์. สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://www.etda.or.th/Useful-Resource/knowledge-sharing/articles/IFBL/FakeNews.aspx>

สุวัชรียा จันทร์บัว. (2566, เมษายน 1). ศูนย์ชั่วร์ก่อนแชร์ สำนักข่าวไทย อสมท. <https://tna.mcot.net/sureandshare-1145927>

เสาวภาคย์ รัตนพงศ์. (2567, มีนาคม 28). ศูนย์ชั่วร์ก่อนแชร์ สำนักข่าวไทยอสมท. <https://tna.mcot.net/sureandshare-1342212>

อุกฤษฎ์ ตั้งสีบกุล และ บริวตร จันทร์เรือง. (2566). **Prompt คืออะไร? และมีความสำคัญในการใช้งาน AI อย่างไร?**. สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://citly.me/2QLf6>

Apple Developer i. (2567). **Passkeys**. Retrieved June 5, 2567, from <https://developer.apple.com/passkeys/>

Apple Support. (2567). **Use passkeys to sign in to apps and websites on iPhone**. Retrieved June 5, 2567, from <https://support.apple.com/en-my/guide/iphf538ea8d0/ios>

AuthenticID. (2567). **Digital Identity**. Retrieved June 4, 2567, from <https://www.authenticid.com/glossary/digital-identity/>

Bunrome R Panyagoon. (2555). **เทคโนโลยีการสื่อสาร**. สืบค้นเมื่อ 4 มิถุนายน 2567, จาก <https://www.gotoknow.org/posts/308385>

Claire Wardle. (2560). **Fake news. It's complicated.** Retrieved June 6, 2567, from <https://firstdraftnews.org/articles/fake-news-complicated/>

Data Cafe Thailand. (2566). **5 Steps เขียน Prompt ยังไงให้ AI เข้าใจเรามากที่สุด.** สืบค้นเมื่อ 23 มิถุนายน 2567, จาก <https://citly.me/sHd2p>

Ekaterina Olshannikova, Thomas Olsson, Jukka Huhtamäki and Hannu Kärkkäinen. (2560). Conceptualizing Big Social Data. **Journal of Big Data**, 4(1), 1-19.

Forbes Coaches Council. (2564). **12 Reasons To Research A Job Applicant's 'Digital Footprint'.** Retrieved <https://www.forbes.com/sites/forbescoachescouncil/2021/02/04/12-reasons-to-research-a-job-applicants-digital-footprint/?sh=50e758b27259>

Indrajeet Deshpande. (2564). **What Is Customer Data? Definition, Types, Collection, Validation and Analysis.** Retrieved June 4, 2567, from <https://www.spiceworks.com/mar-keting/customer-data/articles/what-is-customer-data/>

Kaspersky. (2567). **What is a digital footprint? And how to protect it from hackers.** Retrieved June 5, 2567, from <https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>

Ladan Nikravan Hayes. (2561). **More Than Half of Employers Have Found Content on Social Media That Caused Them NOT to Hire a Candidate, According to Recent CareerBuilder Survey.** Retrieved June 5, 2567, from <https://citly.me/sJzop>

MGR Online. (2566). **สดช.เผยแพร่คนไทยออนไลน์ 7 ชั่วโมง 25 นาที 89.5% เข้าถึงอินเทอร์เน็ต.** สืบค้นเมื่อ 13 มิถุนายน 2567, จาก <https://mgonline.com/cyberbiz/detail/9660000077412>

Nikita Toshi. (2567). **Phone Time And Overall Health – What's The Optimal Screen Time?.** Retrieved June 5, 2567, from <https://pharmeasy.in/blog/phone-time-and-overall-health-whats-the-optimal-screen-time/>

Per Christensson. (2557). **Digital Footprint.** Retrieved June 5, 2567, from https://techterms.com/definition/digital_footprint

Prompt Engineering Guide. (2567). **Prompt Engineering Guide.** Retrieved June 6, 2567, from <https://www.promptingguide.ai/>

Sahatorn Petvirojchai. (2564). **Digital Footprint คืออะไร? ทำไง HR ใช้คัดเลือกพนักงานได้.** สืบค้นเมื่อ 6 มิถุนายน 2567, จาก https://th.hrnote.asia/recruit/digital-footprint-210630/#12_Digital_Footprint_HR

UNESCO Institute of Statistics. (2567). **Digital literacy.** Retrieved June 7, 2567, from <https://uis.unesco.org/en/glossary-term/digital-literacy>

Wikipedia. (2567). **Etiquette in technology.** Retrieved June 5, 2567, from https://en.wikipedia.org/wiki/Etiquette_in_technology

World Economic Forum. (2566). **The Future of Jobs Report 2023.** Retrieved June 5, 2567, from <https://www.weforum.org/publications/the-future-of-jobs-report-2023/>



ทีมพัฒนาหลักสูตร และสนับสนุนโครงการฯ



สำนักงานพัฒนาธุกรรมทางอิเล็กทรอนิกส์

อัจฉราพร หมุดระเด่น

กริช ขาวอุปถัมภ์

ชนนิกานต์ คงสุวรรณ

จิรายุทธ์ กุลพฤกษ์

นาพร สีสถาด

ที่ปรึกษา



ผศ.ดร.เจษฎา ศาลาทอง

คณบดีคณะศศิศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ดร.ปรัชญ์ ส่งจาม

คณบดีวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

ดร.ดารุวรรณ ศรีแก้ว

คณบดีคุณศาสตร์อุทศาสตร์และเทคโนโลยี

มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

นิธิภัทร ศรีอัญญา

ผู้อำนวยการสถาบันพัฒนาบุคลากรดิจิทัล

สถาบันพัฒนาบุคลากรดิจิทัล กรมพัฒนาฝีมือแรงงาน กระทรวงแรงงาน



กองบรรณาธิการ



ศุนย์ข่าวรัฐสภา บริษัท อสมท จำกัด (มหาชน)

พิรพล อนุตรโสตถี

จิรชยา นวลนิมณ้อย

อัครมณี ระวีแสงสุรย์

ยศวดี จิตบำรรัศมี

จิราภา อ่อนเกลี้ยง

จิราพัชร สุวรรณพันธ์

กฤษณา กาญจนเพ็ญ

เสาวภาคย์ รัตนพงศ์

ชยานินธ์ ผ่องใส

กัลย์ธิรา ตันเสดียร

ณัฐพลด อินทร์สวัสดิ์

เบญญาภา วรรธนาชีพ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
โทรศัพท์ : 02 123 1234 | โทรสาร : 02 123 1200

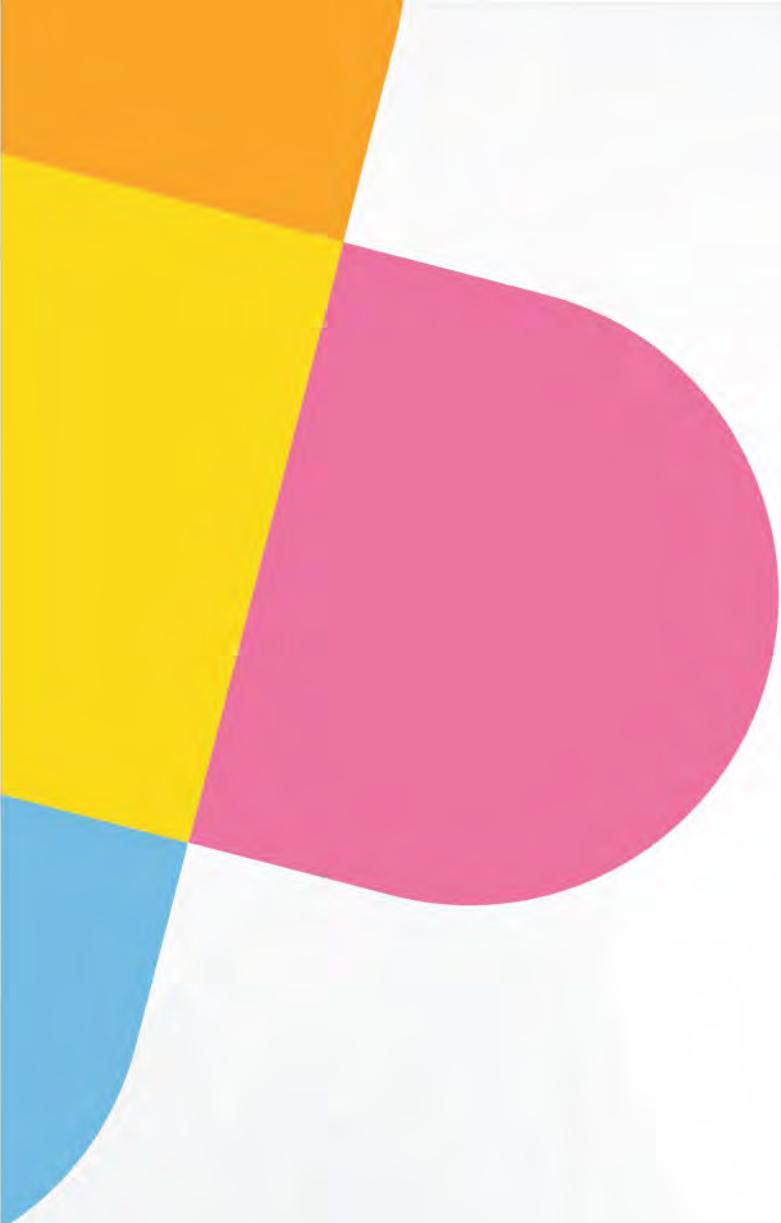


: ETDA THAILAND



ETDA





สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

โทรศัพท์ : 02 123 1234 | โทรสาร : 02 123 1200



: ETDA THAILAND

