



**EDDC** *Plus*  
ETDA DIGITAL CITIZEN



# คู่มือ การสร้าง ความตระหนักรู้ ในการใช้อินเทอร์เน็ต

ETDA DIGITAL CITIZEN PLUS





คู่มือ  
การสร้าง  
ความตระหนักรู้  
ในการใช้อินเทอร์เน็ต  
ETDA DIGITAL CITIZEN PLUS

สแกนเพื่อเข้าสู่  
หลักสูตรออนไลน์



# คู่มือ การสร้าง ความตระหนักรู้ ในการใช้อินเทอร์เน็ต

ETDA DIGITAL CITIZEN PLUS

พิมพ์ครั้งแรก กรกฎาคม 2567

สงวนลิขสิทธิ์ โดย : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

Electronic Transactions Development Agency

## ข้อมูลทางบรรณานุกรมของหอสมุดแห่งชาติ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์.

คู่มือการสร้างความตระหนักรู้ในการใช้อินเทอร์เน็ต ETDA DIGITAL CITIZEN PLUS.--

กรุงเทพฯ : สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, 2567.

362 หน้า.

1. เทคโนโลยี -- แห่งสังคมวิทยา. 2. อินเทอร์เน็ต -- แห่งสังคม. I. ชื่อเรื่อง.

303.483

ISBN 978-616-7956-63-3

## จัดพิมพ์โดย

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา (อาคารบี)

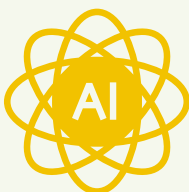
ชั้นที่ 6 เลขที่ 120 หมู่ที่ 3 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง

เขตหลักสี่ กรุงเทพมหานคร 10210

โทรศัพท์ : 02 123 1234 โทรสาร : 02 123 1200

## พิมพ์ที่

บริษัท พีดับบลิว พรินติ้ง จำกัด



# แนะนำการใช้คู่มือ



ยกระดับทักษะ  
ความฉลาดทางดิจิทัลทั้ง 5 ด้าน

หน้า 1 - 45



**ด้านที่ 1**  
อัตลักษณ์ดิจิทัล  
Digital Identity



หน้า 46 - 117



**ด้านที่ 2**  
การใช้เทคโนโลยีดิจิทัล  
อย่างเหมาะสม  
Digital Use



หน้า 118 - 167



**ด้านที่ 3**  
การจัดการ  
ความปลอดภัย  
ในโลกดิจิทัล  
Digital Security



หน้า 168 - 232



**ด้านที่ 4**  
การสื่อสารดิจิทัล  
Digital  
Communication



หน้า 233 - 337



**ด้านที่ 5**  
การรู้เท่าทันดิจิทัล  
Digital Literacy



# สัญลักษณ์พิเศษที่ใช้ในคู่มือ

เพื่อช่วยในการเลือกเนื้อหา หรือระบุถึงความสำคัญ และความพิเศษของเนื้อหา คู่มือเล่มนี้จึงได้มีการทำเครื่องหมายด้วยสัญลักษณ์ไอคอนตามคุณสมบัติของข้อมูล ดังต่อไปนี้



สัญลักษณ์นี้หมายถึง

ประเด็นหรือข้อมูลที่สำคัญ ควรจดจำให้ดี



สัญลักษณ์นี้หมายถึง

เคล็ดลับ คำแนะนำต่าง ๆ ที่มีประโยชน์  
ควรนำไปปรับใช้



**WARNING**

สัญลักษณ์นี้หมายถึง

ป้ายเตือนภัย ที่ควรใส่ใจระมัดระวัง  
ถึงผลกระทบ ความเสี่ยง  
และอันตราย ที่อาจตามมา



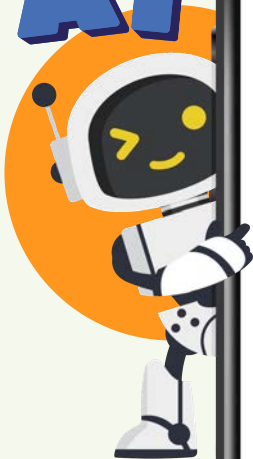
สัญลักษณ์นี้หมายถึง

ประเด็นหรือข้อมูลที่ต้องการยกตัวอย่าง  
เพื่อให้ผู้อ่านเข้าใจในเนื้อหามากยิ่งขึ้น



# คำนำ

# AI



“ขอคำนำสำหรับคู่มือ EDC Plus เล่มนี้แบบสั้น ๆ”

AI : “คู่มือเล่มนี้เป็นแหล่งความรู้และแนวทางสำหรับ "First Jobber" ในระดับพื้นฐาน เพื่อพัฒนาทักษะดิจิทัลทั้ง 5 ด้าน ตามหลักสูตร ETDA Digital Citizen (EDC) ฉบับปรับปรุงใหม่ เพื่อให้พร้อมรับมือ กับ โลกการทำงานยุคดิจิทัล เนื้อหาภายในครอบคลุมตั้งแต่ พื้นฐานการใช้งาน เทคโนโลยีดิจิทัล การรู้เท่าทันสื่อ ไปจนถึงการใช้ประโยชน์จากเทคโนโลยีดิจิทัล เพื่อการทำงานและพัฒนาตนเอง”



+ ข้อความ

จากบทสนทนาจริงข้างต้น ที่เราขอให้ AI รายหนึ่งช่วยเขียนคำนำคู่มือเล่มนี้ออกมา ภายใน 3 วินาที เป็นหลักฐานเชิงประจักษ์ที่ชัดเจนว่า การใช้ชีวิตในยุคดิจิทัลปัจจุบัน และอนาคต มนุษย์เรากำลังมีความท้าทายมากเพียงใด

อีกทั้งยังมีความท้าทายจากหลากหลายองค์ความรู้เกี่ยวกับเทคโนโลยีดิจิทัลที่ปัจจุบัน กลายเป็น “Minimum Requirements” หรือความรู้จำเป็นขั้นพื้นฐานสำหรับคนทำงานและทุกคนที่เกี่ยวข้องกับเทคโนโลยีดิจิทัล



# คำนำ



- การรู้จักปกป้องดูแลตัวตนบนโลกดิจิทัล ไม่ให้เสื่อมเสีย และไม่ถูกสวมรอยขโมยตัวตน
- การรู้จัก “ใช้งาน” ไม่ใช่ “ถูกใช้งาน” โดยอุปกรณ์ดิจิทัล บริการดิจิทัล หรือสังคมดิจิทัล
- เราจะปกป้องทรัพย์สินและสิ่งมีค่าของเราและองค์กร ท่ามกลางการโจมตีทางไซเบอร์ที่ลึกลับได้อย่างไร
- “เจ็บใจ เจ็บปวด อย่างที่ไม่เคยรู้สึกมาก่อนเพราะโลกดิจิทัลหรือเปล่า?” จริง ๆ แล้วเราควรจัดการและจำกัดการเปิดรับและส่งสารอย่างไร
- ในยุคที่เราต้องพึ่งพาข้อมูลมากขึ้น แต่ความเชื่อถือได้ กลับยิ่งถดถอยน้อยลง เราควรรับมืออย่างไร
- ที่สำคัญ เราต้องเตรียมตัวอย่างไร เมื่อยุคแห่ง AI มาถึงอย่างเต็มที

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

คุณไม่จำเป็นต้องอ่านเรียงกันตั้งแต่ต้นจนจบ ขอให้เริ่มต้นที่เรื่องที่ใกล้ตัวและสนใจที่สุด เพราะคู่มือเล่มนี้เป็นของคุณ คุณสามารถย้อนกลับมาอ่านเพิ่มเติมได้ทุกเมื่อ

ยิ่งไปกว่านั้น คุณสามารถใช้คู่มือเล่มนี้ ประกอบกับ หลักสูตรออนไลน์เรียนฟรี EDC Plus ซึ่งหยิบย่อนเนื้อหาแนะนำเสนอด้วยรูปแบบที่เข้าใจง่ายขึ้น ภายในเวลาไม่ถึง 3 ชั่วโมง พร้อมมอบวุฒิบัตรดิจิทัลเป็นหลักฐานแห่งการเรียนรู้และผ่านการทดสอบ

หากพร้อมแล้วที่จะยกระดับ “ทักษะความฉลาดทางดิจิทัล” ไปด้วยกัน ขอเชิญคลิกเข้าสู่เนื้อหา EDC Plus ในหน้าถัดไปได้ทันที

**ด้วยความปรารถนาดี**

**สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA)**

# คำนิยม

## EDC TRAINER รุ่น 1

คุณวัช - วชิรา พงศ์พยัคฆ์

EDC ให้ความรู้ในการรับมือกับโลกดิจิทัลที่กำลังเป็นส่วนหนึ่งของชีวิต ได้ทั้งประโยชน์และปรับเรื่องราวไปใช้ได้ เหมาะกับคนทุกวัย โดยเฉพาะกลุ่มสูงวัย ที่ต้องออกไปเป็นกิจกรรมสนุก ๆ ให้โลกดิจิทัลเป็นเรื่องที่ไม่น่ากลัวเลย

คุณเฮง - เดชฤทธิ์ สีหาราช

EDC ถือเป็นหลักสูตรที่ยกระดับทักษะและศักยภาพทางด้านดิจิทัล ทั้ง 5 ด้าน ให้กับตัวผมได้เป็นอย่างดี สามารถนำไปต่อยอดได้ในชีวิตประจำวัน ซึ่งสอดคล้องกับสถานการณ์ของโลกในยุคปัจจุบัน ที่เปลี่ยนแปลงไป

# คำนิยาม



## EDC TRAINER รุ่น 2

### คุณตุ๊ก - ศิริรัตน์ กุญชรจันทร

ขอขอบคุณโครงการ EDC Trainer ที่ได้จัดขึ้นมาเพื่อหาแนวร่วมในการช่วยกันส่งต่อความรู้ ความเข้าใจในการใช้สื่ออย่างปลอดภัย และเป็นประโยชน์ต่อสังคมอย่างมาก ช่วยยกระดับคุณภาพชีวิตของประชาชนและสร้างความยั่งยืนให้กับพลเมืองในยุคดิจิทัลนี้

### คุณต๋อง - สุนันต์ จิรพัฒนพร

อบรม EDC แล้ว เมื่อต้องส่งต่อความรู้ต่อไปผมเปรียบตัวผมให้เป็นเหมือน GPS ที่คอยแนะนำเส้นทางในการใช้งานด้านดิจิทัล ได้ถูกต้องเหมาะสม รู้ทันก้าวทันโลก ช่วยให้คนไทยไม่หลงทางในยุคดิจิทัล

### คุณแพรว - นิชชา บุตรดีสุวรรณ

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

# สารบัญ

<b>ด้านที่ 1 อัตลักษณ์ดิจิทัล (Digital Identity)</b>	<b>1</b>
<b>1.1 Digital Citizen Identity</b> .....	<b>7</b>
เพราะทุกคนล้วนมีโลกอีกใบ .....	8
แล้วอะไร คือสิ่งที่แสดงตัวตนของเราในโลกดิจิทัล ? .....	9
รู้ได้อย่างไร ใครเป็นเจ้าของอัตลักษณ์ ? .....	11
Biometrics สิ่งที่ใช้แยกแยะตัวตนของแต่ละบุคคล .....	12
อัตลักษณ์ดิจิทัลในทางบวก = อัตลักษณ์ทางบวกในชีวิตจริง .....	13
ผลจากการสร้างอัตลักษณ์ทางดิจิทัล .....	14
How to 3 STEP ในการปรับปรุงอัตลักษณ์ดิจิทัล .....	16
สวดแล้วปัง ! คาถา 8 ข้อ เสริมชีวิต สร้างอัตลักษณ์ดิจิทัลที่ดี ในสังคมดิจิทัล	18
BEST PRACTICES แนวปฏิบัติที่ดีในการจัดการอัตลักษณ์ดิจิทัล .....	19
<b>1.2 Digital Privacy</b> .....	<b>23</b>
ความเป็นส่วนตัวในโลกดิจิทัล (สิ่งมีค่าที่เราอาจหลงลืมไป) .....	24
รู้ทันภัย และความเสี่ยง หากไม่ดูแลข้อมูลส่วนตัวให้ดี .....	26
ปัญหาภัยคุกคามและละเมิดความเป็นส่วนตัว .....	28
การจัดการความเป็นส่วนตัวในโลกดิจิทัล .....	32
กฎหมายที่น่าสนใจ และควรรู้ไว้ .....	39

# สารบัญ

<b>ด้านที่ 2 การใช้เทคโนโลยีดิจิทัลอย่างเหมาะสม (Digital Use)</b>	<b>47</b>
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 เพื่อสร้างค่านิยมเชิงบวกต่อชุมชนและพัฒนาคุณภาพชีวิต	98
การสืบค้นข้อมูลจากสื่อดิจิทัล	104
<b>ด้านที่ 3 การจัดการความปลอดภัยในโลกดิจิทัล (Digital Security)</b>	<b>119</b>
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

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

# สารบัญ

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



01



# อัตลักษณ์ดิจิทัล



## Digital Identity

# แนะนำสำหรับผู้สอน



## • วัตถุประสงค์

ผู้เรียนมีความรู้ และสามารถอธิบายถึง ความสำคัญของอัตลักษณ์ดิจิทัล ความเป็นส่วนตัว และจริยธรรมในโลกดิจิทัลได้

## • ขอบเขตของเนื้อหาเรื่องนี้

### 1.1 Digital Citizen Identity



โลกดิจิทัล

วันที่สอน  
...../...../.....



อัตลักษณ์ดิจิทัลคืออะไร ?

วันที่สอน  
...../...../.....



กระบวนการการระบุตัวตน พิสูจน์ และยืนยันตัวตน

วันที่สอน  
...../...../.....



Biometrics สิ่งที่ใช้แยกแยะตัวตนของแต่ละบุคคล

วันที่สอน  
...../...../.....



การสร้างอัตลักษณ์ดิจิทัล

วันที่สอน  
...../...../.....



ผลจากการสร้างอัตลักษณ์ทางดิจิทัล

วันที่สอน  
...../...../.....



การปรับปรุง และแนวปฏิบัติที่ดีในการจัดการอัตลักษณ์ดิจิทัล

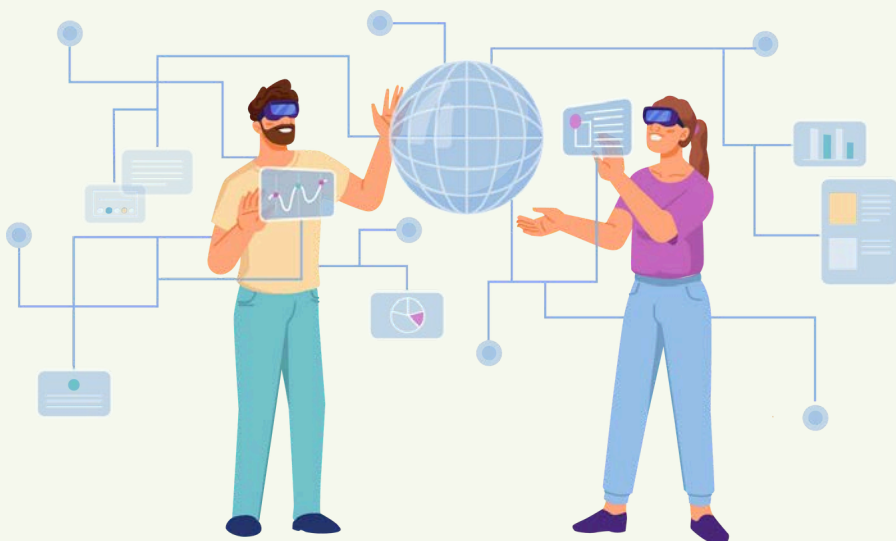
วันที่สอน  
...../...../.....

## • ขอบเขตของเนื้อหาตอนนี้

### 1.2 Digital Privacy

- ความเป็นส่วนตัวในโลกดิจิทัล วันที่สอน  
...../...../.....
- รู้ทันภัย และความเสียหาย หากไม่ดูแลข้อมูลส่วนตัวให้ดี วันที่สอน  
...../...../.....
- การจัดการความเป็นส่วนตัวในโลกดิจิทัล วันที่สอน  
...../...../.....
- กฎหมายที่น่าสนใจ และควรรู้ไว้ วันที่สอน  
...../...../.....

เวลาในการเรียน



# รู้ศัพท์

## ไม่ลับสน



1



### TOXIC SOCIETY

สภาพแวดล้อมทางสังคมที่มักจะมีการกระทำ ความคิด หรือการแสดงออก ที่ส่งผลต่อ คนในสังคม ซึ่งอาจจะส่งผลต่อสุขภาพจิต สภาพจิตใจ ความสัมพันธ์ ตลอดจนคุณภาพชีวิต โดยอาจจะเกิดจากการไม่ให้เกิดเกียรติผู้อื่น การแข่งขันที่ไม่สร้างสรรค์ การมองโลกในแง่ร้าย หรือการปิดกั้นความคิดเห็นของผู้อื่น

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 หรือกรอกช้ากว่าเวลาที่กำหนด การเข้าระบบนั้น ก็จะไม่สำเร็จ

4



### ROMANCE SCAM

คือ การหลอกให้หลงรัก หลอกให้เชื่อว่ารัก หลอกให้เชื่อใจ และใช้ความรักความเชื่อใจ หรือความหวังของเหยื่อ เพื่อแสวงหาประโยชน์

# รู้ศัพท์

# ไม่ลับสน



5



## HYBRID SCAM

คือ การหลอกลงงที่ผสมผสานระหว่าง  
ความรัก และการลงทุน  
หลอกให้เชื่อใจ ไว้วางใจ แล้วชวนลงทุน

6



## REMOTE ACCESS SCAM

คือ หลอกให้รักแล้วกดลิงก์ ดาวโหลด  
แอปพลิเคชันรีโมต ควบคุมสมาร์ตโฟน  
และทำการดูดเงินในบัญชี

7



## SEXTORTION

การขู่กรรโชกทางเพศ เริ่มต้นด้วยการ  
เข้ามาขอเป็นเพื่อนผ่านช่องทางต่าง ๆ  
และชวนทำกิจกรรมทางเพศผ่านทางออนไลน์  
จากนั้น มีฉฉฉฉจะบันทึกภาพ วิดีโอดังกล่าวไว้  
แล้วนำมาข่มขู่ภายหลัง



ถ้าคุณเรียนผ่านด้านนี้  
คุณจะสามารถ  
รักษาได้ทั้งข้อมูลส่วนตัว  
และ ทรัพย์สิน

## 1.1

# DIGITAL CITIZEN IDENTITY

## วัตถุประสงค์

1. ผู้เรียนอธิบายถึงการสร้างอัตลักษณ์ดิจิทัลของตนเองให้เหมาะสมได้
2. ผู้เรียนตระหนักถึงความสำคัญของอัตลักษณ์ดิจิทัล
3. ผู้เรียนตระหนักถึงผลกระทบที่จะเกิดขึ้นจากการสร้างอัตลักษณ์ดิจิทัล ทั้งเชิงบวกและลบได้
4. ผู้เรียนสามารถเข้าใจถึงพฤติกรรมที่แสดงออกถึงการมีจริยธรรมในโลกดิจิทัลได้





# เพราะทุกคน ล้วนมีโลกอีกใบ



## รู้หรือไม่ ?

REMEMBER

“เราทุกคนล้วนมีโลกอีกใบ” ประโยคนี้ ฟังดูแล้ว ก็อาจชวนสร้างรอยร้าวให้กับหลายบ้านได้ แต่สำหรับบริบทนี้ โลกอีกใบ ที่กำลังหมายถึงคือ โลกเสมือน ที่เราทุกคนสร้างขึ้นมากู่ขนานกับโลกความจริงที่เราอยู่อาศัยหรือเรียกว่า “โลกดิจิทัล” โดยโลกใบนี้ จะประกอบด้วยพื้นที่ ผู้คน เครื่องมือ ทรัพยากร และกิจกรรมที่คล้ายกับโลกความจริง เพียงแต่ถูกสร้างขึ้นจากอุปกรณ์อิเล็กทรอนิกส์ และดำรงชีพผ่านออนไลน์นั่นเอง ซึ่งก่อนที่เราจะเป็นพลเมือง หรือผู้คนในโลกดิจิทัลได้นั้น เราต้องทำการสมัครเข้าใช้งาน ยอมรับเงื่อนไขในการเข้าสู่พื้นที่แต่ละแห่งในโลกดิจิทัลก่อน เพื่อให้เรามีตัวตนบนโลกใบนี้ แล้วจึงจะสามารถสร้าง หรือทำกิจกรรมต่าง ๆ ได้ ไม่ว่าจะเป็น

ติดต่อสื่อสาร



แบ่งปัน  
ข้อมูลข่าวสาร

ใช้บริการ  
หน่วยงานภาครัฐ  
และเอกชน



ทำธุรกรรม  
ทางการเงิน

# อะไรคือ สิ่งที่แสดงตัวตน ของเราในโลกดิจิทัล ?



## REMEMBER

เมื่อเราอวตารสร้างชีวิตขึ้นมาอยู่บนโลกดิจิทัลแล้วนั้น อีกคำถามที่ตามมาคือ “แล้วอะไรคือ สิ่งที่แสดงออกถึงตัวตนของเรา เมื่ออยู่ในโลกดิจิทัล ?” สิ่งนั้นเรียกว่า **อัตลักษณ์ดิจิทัล** หรือสิ่งที่บ่งบอกความเป็นตัวเรา ลักษณะเฉพาะบุคคลของเรา และภาพลักษณ์ที่แสดงออกให้ผู้อื่นรับรู้ ซึ่งเกิดจากข้อมูลที่ใส่หรือโพสต์ลงบนโลกดิจิทัล โดยหากใครพบเห็น ก็จะสามารถจดจำ และใช้ระบุตัวตนของเราได้

## 3 องค์ประกอบหลัก ปกมุดอัตลักษณ์ดิจิทัล

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 หรือนามสกุล ชื่อเล่น ตำแหน่งที่อยู่ ประเทศ รหัสไปรษณีย์ เพศ เผ่าพันธุ์ เชื้อชาติ กลุ่มอายุ อาชีพ ประวัติการทำงาน การศึกษา วันเดือนปีเกิด

# 2

## Social & Behavioral Information

ข้อมูลทางสังคม และข้อมูลเชิงพฤติกรรมการใช้งาน เช่น ความสัมพันธ์กับบุคคลอื่น ความสนใจ ทักษะ ทักษะ ทักษะ ลักษณะนิสัย การแสดงออก

# 3

## Digital Information

ข้อมูลทางดิจิทัล เช่น บัญชีและรหัสผ่านแพลตฟอร์มต่าง ๆ ประวัติการใช้งานอินเทอร์เน็ต ข้อมูลการเข้าถึงเว็บไซต์ โพสต์บนโซเชียลมีเดีย

# รู้ได้อย่างไร ใครเป็น เจ้าของอัตลักษณ์ ?



การจะบอกได้ว่า ใครคือเจ้าของอัตลักษณ์นั้น ควรที่จะผ่านกระบวนการการระบุตัวตน พิสูจน์ และยืนยันตัวตนที่มีระดับความน่าเชื่อถือก่อน

## การระบุตัวตน (Identification)



คือขั้นตอนที่ผู้ใช้แสดงตนว่าเป็นใคร มีอัตลักษณ์ดิจิทัลใด เช่น การกรอกชื่อผู้ใช้

## พิสูจน์ตัวตน (Identity Proofing)



คือ ขั้นตอนรวบรวม และตรวจสอบความเชื่อมโยงระหว่างบุคคลกับอัตลักษณ์นั้น เพื่อให้มั่นใจว่าอัตลักษณ์นั้นเป็นของคนนั้นจริง

## ยืนยันตัวตน (Authentication)



คือขั้นตอนการยืนยันอัตลักษณ์ของบุคคล ด้วยการตรวจสอบสิ่งที่ใช้ยืนยันตัวตน เช่น รหัสผ่าน OTP Biometric เป็นต้น



# Biometrics

## สิ่งที่ใช้แยกแยะตัวตนของแต่ละบุคคล

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

### 1 ลักษณะทางสรีรวิทยา (Physiological Characteristics)

เป็นสิ่งที่มองเห็นได้โดยตรงจากส่วนต่าง ๆ ของร่างกาย เช่น ใบหน้า ม่านตา ลายนิ้วมือ ดีเอ็นเอ (DNA)



ลักษณะทางสรีรวิทยานั้น มักจะถูกนำไปใช้ในระบบการพิสูจน์ตัวตน (Identify) เพื่อยืนยันว่าเราเป็นบุคคลนั้นจริง ๆ เช่น การเปิดบัญชีหรือทำธุรกรรมทางการเงินบนแอปพลิเคชัน ที่ใช้การใส่ใบหน้า หรือลายนิ้วมือในการยืนยันตัวตน

## 2

### ลักษณะเฉพาะทางพฤติกรรม (Behavioral Characteristics)

เป็นสิ่งที่วัดจากการกระทำ หรือพฤติกรรมการแสดงออกของแต่ละบุคคล เช่น เสียงพูด ลายเซ็น ลักษณะการเดิน การพูด

## อัตลักษณ์ดิจิทัลในทางบวก

=

## อัตลักษณ์ทางบวกในชีวิตจริง

จะเห็นได้ว่า อัตลักษณ์ดิจิทัลนั้น เป็นสิ่งสำคัญอย่างมากในการใช้ชีวิตบนโลกดิจิทัลของเรา ดังนั้น เราจึงควรมีการสร้างอัตลักษณ์ดิจิทัลที่ดี ทั้ง 3 องค์ประกอบ

### 1 Personally identifiable information

เน้นการดูแล ปกป้องให้ปลอดภัย เพื่อป้องกันไม่ให้เสียงโดนสวมรอยขโมยตัวตนจากบุคคลอื่น เช่น ไมโพสต์เปิดเผยข้อมูลส่วนบุคคลต่าง ๆ ที่สำคัญในอินเทอร์เน็ต หรือให้ข้อมูลกับบุคคลที่ไม่น่าเชื่อถือ หรือควรตั้งค่าความเป็นส่วนตัวในบัญชีออนไลน์ต่าง ๆ เพื่อจำกัดวงผู้อ่าน หรือนำข้อมูลไปใช้

### 2 Social & Behavioral Information

เน้นการสร้างสรรค์ และแสดงออกอย่างเหมาะสม

### 3 Digital Information

เน้นการจัดการอย่างปลอดภัย ไม่เข้าเว็บไซต์ที่ไม่น่าเชื่อถือ เว็บพนันหรือเว็บโคจร ไม่สร้างร่องรอยดิจิทัลอันต่างพร้อย

# ผลจากการสร้าง อัตลักษณ์ทางดิจิทัล



**ผลลัพธ์**

**สุดว้าว** การสร้างอัตลักษณ์ดิจิทัลที่ดี



01



## ภาพจำที่แสนเลิศ

ผู้คนจดจำเราในทางที่ดี เพราะการจดจำในทางที่ดีจะส่งผลต่อการใช้ชีวิตในโลกความเป็นจริง ทั้งในปัจจุบันและอนาคต

## เปิดโอกาสให้ตัวเอง

02



หากเราสร้างเนื้อหาที่ดีที่ผู้คนชื่นชอบใจฟุ้งก็จะมีคนเข้ามาติดตามเรามากขึ้น สิ่งนี้เปิดโอกาสให้พวกเรามากมาย ตั้งแต่ได้รับการชื่นชม ได้มีโอกาสเข้าร่วมกิจกรรมใหม่ ๆ สร้างสังคมใหม่ ๆ หรืออาจนำไปสู่การสร้างรายได้ในรูปแบบของ Content creator ได้

03



## แบ่งปันสังคมดิจิทัลที่น่าอยู่

สร้างสภาพแวดล้อมบนโลกออนไลน์ ในเชิงสร้างสรรค์ ช่วยเหลือและสอดส่องภัยที่เกิดขึ้น ทำให้ลดปัญหาการโจรกรรมทางดิจิทัล สะท้อนผลกระทบในเชิงบวกกลับมาถึงโลกของความเป็นจริงและยังช่วยลดภาวะการเกิด Toxic society ด้วย

ในทางตรงกันข้าม หากเราสร้างอัตลักษณ์ดิจิทัลในทางลบ ก็อาจส่งผล ดังนี้

## ผลรวม

ผลรวม จากอัตลักษณ์ดิจิทัลในทางลบ

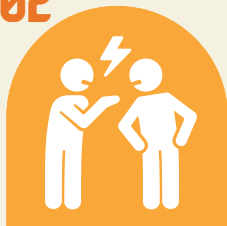
01



### ติดลบด้วยภาพจำ

การถูกจดจำในทางที่ไม่ดี อาจส่งผลเสียมากกว่าที่คิด ตั้งแต่ ปัญหาด้านภาพลักษณ์ ความสัมพันธ์ จนไปถึง โอกาสในหน้าที่การงาน และความน่าเชื่อถือ เช่น ในกรณีนักศึกษาฝึกงาน ได้โพสต์ข้อความด้วยอารมณ์ว่า สถานที่เคยฝึกงานไว้ จึงไม่ได้รับพิจารณาจากที่ทำงาน ที่ไปสมัครงาน เพราะถูกตัดสินจากโพสต์ ที่สะท้อนทัศนคติแง่ลบจนพลาดโอกาส

02



### สุดซ้ำความสัมพันธ์

หากเราสร้างอัตลักษณ์ที่ไม่ดี อาจส่งผลต่อความรู้สึกของคนรอบข้าง เกิดความขัดแย้ง ไม่พอใจกับสิ่งที่เราโพสต์ แชร์ หรือเผยแพร่ ไปจนถึงอาจเกิดการระรานในโลกดิจิทัลผ่านช่องทางต่าง ๆ ด้วยการใช้อภัยคำเสียดสี จนทำให้เกิดความไม่สบายใจ

03



### รู้ไม่ทัน ถูกโจรกรรมข้อมูล

หากเราเผยแพร่ข้อมูล หรือเก็บรักษาอัตลักษณ์ไม่ดี ผู้ประสงค์ร้าย หรือมีเจตนาชั่วอาจใช้อัตลักษณ์ของเราในการโจรกรรมข้อมูล หลอกหลวง หรือละเมิดความเป็นส่วนตัว



# มาจัดการ อัตลักษณ์ดิจิทัลกันเถอะ !

ก่อนอื่นถ้าหากเราจำไม่ได้ว่า เราเคยทำอะไร ที่จะทำให้เกิด  
อัตลักษณ์ดิจิทัลที่ไม่ดีไว้หรือไม่ ? ให้ลองมาตรวจสอบด้วยวิธีนี้

## How to 3 STEP

### ในการปรับปรุงอัตลักษณ์ดิจิทัล

STEP

1

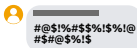


#### ค้นหาชื่อ และข้อมูลบนโลกดิจิทัล

ให้พิมพ์ชื่อจริง หรือชื่อ Account ที่ต้องการค้นหา  
บน Google

STEP

2



#### ลบข้อมูลด้วยตัวเองง่ายนิดเดียว

ไล่มองหาอัตลักษณ์ดิจิทัลที่ไม่ต้องการให้คนอื่นเห็น  
จากผลลัพธ์ที่ขึ้นมา จากนั้นเข้าไปทำการลบ หาก  
ไม่สามารถดำเนินการลบได้ด้วยตัวเอง ให้ทำการกด  
รีพอร์ต หรือติดต่อเข้าไปที่ผู้ดูแล หรือผู้ให้บริการ  
เพื่อติดต่อขอความช่วยเหลือ

STEP

3



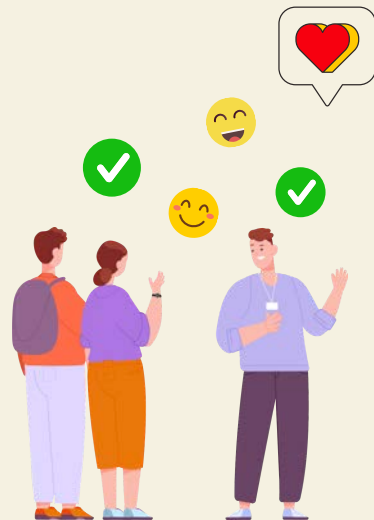
#### เริ่มต้นใหม่ ใส่ใจอัตลักษณ์

เมื่อรู้แล้วว่า ต้องมีอะไรผิดพลาดตรงไหน ควรทำ  
ความเข้าใจ หลีกเลียงไม่ให้เกิดขึ้นอีกครั้ง และสร้าง  
อัตลักษณ์ดิจิทัลต่อจากนี้ให้ดี



## ชีวิตที่ดี เริ่มจากสังคมที่น่าอยู่

ในยามที่เรานั้น มีตัวตนบนโลกไม่ว่าจะเป็นโลกความจริง หรือโลกดิจิทัล เราย่อมถือเป็นสมาชิกคนหนึ่งในสังคม เป็นพลเมืองในสังคมนั้น และสังคมจะเป็นเช่นไร ก็ย่อมส่งผลต่อคุณภาพชีวิตของเราด้วย ดังนั้น หากเราอยากมีคุณภาพชีวิตที่ดี เราก็ควรมีความเข้าใจ และปฏิบัติตนให้เหมาะสม เพื่อสร้างสังคมให้น่าอยู่ไปด้วยกัน หรือในทางโลกดิจิทัล อาจหมายถึง การมีจริยธรรมพลเมืองดิจิทัล นั่นเอง





TIP

## สวดแล้วปัง !



### คาถา 8 ข้อ เสริมชีวิต สร้างอัตลักษณ์ดิจิทัลที่ดี

#### 1. คิดก่อนโพสต์

ควรเน้นการโพสต์แชร์ข้อมูลหรือเนื้อหาที่สร้างสรรค์และมีประโยชน์

#### 2. มีประโยชน์ถึงแชร์

คิดให้ดีก่อนโพสต์และแชร์เพื่อสร้างภาพจำที่ดีในโลกดิจิทัล

#### 3. ทุให้แน่นอนอย่าใจร้อน

ไม่ใจร้อน ตอบกลับด้วยอารมณ์คิดให้รอบคอบก่อนตอบโต้

#### 4. ใช้ตอนไหน ต้องขอก่อน

ทุกอย่างในโลกออนไลน์มีเจ้าของ จึงต้องระมัดระวังในการนำข้อมูลที่ไม่รู้ที่มาหรือไม่ได้รับอนุญาตไปใช้งาน หากจำเป็นควรมีการอ้างอิง หรือการขออนุญาตก่อนการใช้งาน

#### 5. ไม่ย่อหย่อน กฎชุมชน

ปฏิบัติตามกฎหรือแนวทางปฏิบัติของชุมชนออนไลน์ เช่น กรณีการเข้าร่วมกลุ่มผ่านโซเชียลมีเดียต่าง ๆ ควรปฏิบัติตามแนวทางที่แต่ละกลุ่มได้กำหนดไว้

#### 6. ทุก ๆ คนควรให้เกียรติ

ให้เกียรติเคารพความคิดเห็นของผู้อื่น โดยไม่เลือกว่า เป็นใคร ช่วงอายุใด เพศใด หรือทำอาชีพอะไร

#### 7. อย่าเรียกก้าวร้าวความขัดแย้ง

ระมัดระวังในการแชร์หรือโพสต์ข้อมูลที่อาจทำให้เกิดความขัดแย้ง หรือกระทบกับความรู้สึก โดยเฉพาะเนื้อหาที่เกี่ยวกับความเชื่อ วัฒนธรรม และการเมือง

#### 8. ร่วมแบ่งปันสิ่งดี ๆ

แบ่งปันสิ่งดี ๆ และสร้างสรรค์เพื่อการสร้างภาพลักษณ์ที่ดี ซึ่งจะส่งผลต่อหน้าที่การงาน การเรียนในอนาคต





# BEST PRACTICES

## แนวปฏิบัติที่ดีในการจัดการ อัตลักษณ์ดิจิทัล



1



### ชื่อ - นามสกุล

ใช้ชื่อนามสกุลที่ไม่ทำให้  
ผู้อื่นเสียหาย และไม่ควรใช้  
ชื่อนามสกุลของผู้อื่น

2



### รูปภาพประจำตัว

ไม่ใช่ภาพของผู้อื่นมาเป็น  
รูปภาพประจำตัว  
หรือภาพที่ละเมิดผู้อื่น

3



### ข้อมูลส่วนตัว

ตั้งค่าความเป็นส่วนตัว  
ไม่เผยแพร่ข้อมูล  
ที่ไม่ควรเผยแพร่

4



### ประวัติในการใช้งาน

ตรวจสอบประวัติ  
การใช้งานบนโลกออนไลน์  
เป็นระยะ หลีกเลี่ยงการเข้าถึง  
เนื้อหาที่ไม่เหมาะสมในอนาคต

5



### เนื้อหา ข้อความ รูปภาพที่เผยแพร่

ตรวจสอบก่อน  
ว่าถูกลิขสิทธิ์หรือสร้าง  
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  
ความคิดเห็นในโซเชียลมีเดีย  
หลีกเลี่ยงการแสดง  
ความคิดเห็นที่ไม่เหมาะสม





ตั้งโลกนี้มีอีกใบใช้ชีวิต

เนรมิตตัวตนดิจิทัล

คู่ขนานกับโลกจริงผูกชีวัน

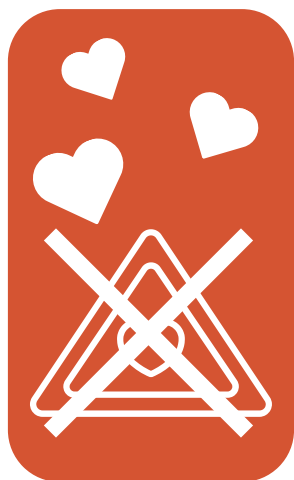
รู้จักกันอัตลักษณ์บอกตัวตน

ตั้งนั้นควรเสริมสร้างภาพที่ดี

ทำให้มีราศีล้วนเป็นผล

แต่ถ้าหากไม่ระวังน่ากังวล

จะยากตนควรพินิจคิดให้ดี



ถ้าคุณเรียนผ่านด้านนี้  
คุณจะเข้าใจความสำคัญ  
ของความเป็นส่วนตัว  
และป้องกันภัยคุกคาม  
ในโลกดิจิทัลได้

## 1.2

DIGITAL  
PRIVACY

## วัตถุประสงค์

1. ผู้เรียนตระหนักถึงความสำคัญของความเป็นส่วนตัว
2. ผู้เรียนสามารถเข้าใจถึงการจัดการข้อมูลส่วนตัวในโลกดิจิทัลได้
3. ผู้เรียนมีความรู้เกี่ยวกับกฎหมายที่เกี่ยวข้อง
4. ผู้เรียนสามารถเข้าใจถึงการแก้ไขปัญหาภาวะคุกคามหรือละเมิดความเป็นส่วนตัว



# สิ่งมีค่า ที่เราอาจหลงลืมไป

การใช้ชีวิตในโลกดิจิทัลนั้น บางครั้งเราก็ลืมห่วงแหนในสิ่งที่เราเห็นคุณค่าในโลกความจริง สิ่งนั้นเรียกว่า "ความเป็นส่วนตัว" เราพยายามหลบเลี่ยงการถูกคนข้าง ๆ ชะเง้อส่องจอมือถือ เราไม่ชอบให้ใครมาแกะกล่องพัสดุที่ส่งมาที่บ้าน หรือเราก็เลือกปิดม่าน ปิดประตู เพื่อรักษาพื้นที่ส่วนตัว แต่หลายคนบนโลกออนไลน์ ก็กลับกลายเป็นเปิดเผยชีวิตทุกซอกทุกมุม และเปิดช่องโหว่ให้คนแปลกหน้า เข้ามาติดตามสอดส่องได้อย่างหายใจรดต้นคอ โดยไม่รู้ตัว และแน่นอนว่า หากเราไม่รักษาความเป็นส่วนตัวให้ดี สิ่งที่เราต้องแลกกับการไม่ดูแลสิ่งมีค่านี้ ก็มีตั้งแต่การถูกละเมิด ถูกแอบอ้าง ถูกสวมรอย ไปจนถึงการต้องรับผิดชอบในสิ่งที่ไม่ได้ก่อ และบางรายอาจนำไปสู่การเสียหายทรัพย์สิน หรือเสียชีวิตได้ ดังนั้น เราจึงต้องมีการควบคุมการเผยแพร่ข้อมูล หรือใช้สิทธิในข้อมูลที่เกี่ยวข้องกับตัวเรา ไม่ยินยอมให้คนที่เราไม่อนุญาต นำข้อมูลนั้นไปถือครองหรือใช้ประโยชน์ นี่คือ "การปกป้องความเป็นส่วนตัว"



**WARNING**



**REMEMBER**

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

โดยข้อมูลส่วนตัวบางข้อมูลเราสามารถเปิดเผยได้ (Personal Information) เช่น ชื่อเล่น นามแฝง อายุ เพศ อาหารที่ชอบ หนังสือโปรด ชื่อสัตว์เลี้ยง

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



WARNING

# รู้ทันภัยและความเสี่ยง หากไม่ดูแลข้อมูลส่วนตัวให้ดี

## โปรดอ่าน ! ถ้าไม่อย่างเสี่ยง

### ลักษณะของความเสี่ยง

ที่อาจจะเกิดขึ้น หากไม่ดูแลข้อมูลส่วนตัวให้ดี อาจเสี่ยงจากการถูกโจรกรรมข้อมูล การถูกหลอกหลวง และการถูกละเมิดความเป็นส่วนตัวได้ เช่น การนำข้อมูลบนเฟซบุ๊กของเราไปแอบอ้าง เพื่อหลอกให้เพื่อนหรือญาติเราโอนเงินให้ หรือเอาข้อมูลเราไปใช้เพื่อหลอก Romance Scam

EXAMPLE

### ยกตัวอย่างข่าว เตือนภัยคนโสด ระวังถูกหลอกให้รักแล้วโอนเงิน



นายประเสริฐ จันทรวงทอง รมว. ดิจิทัลเพื่อเศรษฐกิจและสังคม หรือ ดีอี กล่าวว่า ขอให้ระวังภัยที่อาจจะเกิดขึ้นจากการหลอกให้รักและโอนเงินออนไลน์ (Romance scam) ในรูปแบบต่าง ๆ เช่น มีฉวยชีพเข้ามาทักทายผ่านโซเชียลมีเดีย จากนั้น ขอคุยเป็นเพื่อนและคนรัก

## EXAMPLE

## ยกตัวอย่างข่าว เตือนภัยคนโสด ระวังถูกหลอกให้รักแล้วโอนเงิน

ก่อนที่จะขอให้เหยื่อโอนเงินให้พร้อมหลอกเหยื่อว่า มีความจำเป็นต้องใช้เงินในรูปแบบต่าง ๆ โดยเฉพาะคนโสด ซึ่งจะตกเป็นเป้าหมายของมิจฉาชีพได้ง่าย ผ่านการล่อลวงให้รัก โดยการใช้เทคนิคทางจิตวิทยา สร้างความเชื่อใจระหว่างกัน พอรักแล้วจะชวนลงทุน (Hybrid scam) ชวนกดลิงก์ หรือดาวน์โหลดแอปฯ รีโมต (Remote access scam) ดูดเงินในบัญชี หรือหลอกให้รักแล้วแบล็กเมล (Sextortion) ชูกรรโชกทางเพศ เป็นต้น

“ล่าสุดพฤติกรรมยังขยายไปถึง การหลอกให้กดรับสติ๊กเกอร์วันวาเลนไทน์ฟรี หลอกลวงให้ผู้ใช้ไลน์ใส่ชื่อและรหัสการเข้าใช้ไลน์ รวมถึง ข้อมูลส่วนตัว แล้วนำชื่อ และรหัสการใช้งานของเหยื่อไปทำธุรกรรมต่าง ๆ หรืออาจมีการสวมสิทธิ์เพื่อกระทำความผิด”

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

# ปัญหาภัยคุกคาม



WARNING

และ

# ละเมิดความเป็นส่วนตัว

ในปัจจุบัน มีปัญหาภัยคุกคามความเป็นส่วนตัวทางดิจิทัลในหลากหลายรูปแบบ ดังนี้

## 1

### การลวงให้กดยินยอมหรือตอบรับ

ขั้นตอนแรก ๆ เมื่อติดตั้งแอปพลิเคชัน หรือ สมัครใช้บริการดิจิทัล มักจะมีขั้นตอนการให้กดยินยอม ตกลง อนุญาต ตอบรับ ซึ่งบางครั้งมาในรูปแบบที่ผู้ใช้ไม่ทันได้ตั้งใจพิจารณา เช่น เป็นกล่องข้อความขนาดเล็ก เป็นข้อความเงื่อนไขขนาดยาว เป็นปุ่มที่ง่ายต่อการกดอนุญาต หรือยินยอม ซึ่งบางครั้งอาจเป็นกลลวงเพื่อชักนำให้ผู้ใช้ เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น และอาจถูกนำข้อมูลเหล่านั้นไปใช้ในทางมิชอบ เช่น แอปฯ เงินกู้ขอเข้าถึงอัลบั้มรูปภาพและสมุดรายนชื่อ

## 2

### การหลอกให้กรอกข้อมูลส่วนตัว

เครื่องมือสำคัญที่ใช้ในการหลอกลวง อาจเป็นเทคนิคการสร้างข่าวปลอม เว็บปลอม ข้อมูลลวงที่ดูน่าเชื่อถือ เพียงเพื่อให้เราหลงเชื่อแล้วกรอกข้อมูลส่วนตัวหรืออนุญาตให้เข้าถึง เช่น การแอบอ้างว่าเป็นแบบฟอร์มขอรับเงินจากโครงการของรัฐบาล เป็นต้น

### 3 ทำให้ดีใจ ตกใจ หวาดกลัว ก่อนฉกฉวยข้อมูลส่วนตัว



บางครั้งมีข้อความสั้นส่งมาพร้อมลิงก์ ซึ่งบางคนเห็นแล้วก็อาจจะตกใจและรีบเร่งเข้าไปดำเนินการ โดยไม่ทันได้ตระหนักว่าเป็นกับดักของมิจฉาชีพ

### 4 ภาครธุรกิจละเมิด หรือใช้ข้อมูลส่วนตัวผิดวัตถุประสงค์

ผู้ให้บริการบางรายไม่ปฏิบัติตามมาตรฐาน และกฎหมายการคุ้มครองข้อมูลส่วนบุคคล อาจมีการนำข้อมูลส่วนตัวของเราไปขายต่อ หรือนำไปใช้ผิดวัตถุประสงค์ที่เรายินยอมหรืออนุญาตตั้งแต่ต้น ซึ่งอาจนำมาซึ่งการถูกคุกคามหรือก่อความรำคาญได้

## EXAMPLE

## จากข่าวเรื่อง เตือน ! ระวังแก๊งมิจฉาชีพ แอบอ้าง สปส. หลอกโอนเงิน-ขโมยข้อมูลส่วนตัว



นายบุญสงค์ ทัพชัยยุทธ์ เลขาธิการสำนักงานประกันสังคม กระทรวงแรงงาน ได้ประชาสัมพันธ์เตือนประชาชน เกี่ยวกับแก๊งมิจฉาชีพที่ได้อัปอ้างสำนักงานประกันสังคม สร้างเว็บไซต์และเพจปลอม เพื่อให้ผู้ประกันตนกดลิงก์และขอข้อมูลส่วนตัวและนำไปสวมรอยทำธุรกรรม จนสูญเสียทรัพย์สิน รวมถึง ก่ออาชญากรรมอื่น ๆ ซึ่งอาจทำให้เกิดความเดือดร้อนและยุ่งยากภายหลัง

## EXAMPLE

## WHOSCALL รายงานประจำปี 2566 คนไทยเป็นเหยื่อ SMS หลอกลวงมากที่สุดในเอเชีย



Whoscall ผู้นำด้านแอปพลิเคชันระบุตัวตนสายเรียกเข้าที่ไม่รู้จัก และ ป้องกันสแปม สำหรับสมาร์ตโฟน เผยรายงานประจำปี 2566 พบ มีจฉาชีพก่อวณคนไทยเพิ่มขึ้น 12.2 ล้านครั้ง คนไทยรับข้อความ หลอกลวงมากที่สุดในเอเชียถึง 58 ล้านข้อความ ซึ่งแนบมากับลิงก์ปลอม ลิงก์ขอลือกอินปลอม การดาวนโหลดมัลแวร์ อันตราย และเพจปลอม หลอกขายของหลอกลวง

### คนไทยรับ SMS หลอกลวงมากที่สุดในเอเชีย

Whoscall เผยจำนวนข้อความหลอกลวง เฉลี่ยคนไทย 1 คน ต้องรับ SMS ที่ น่าสงสัย 20.3 ข้อความ ซึ่งมากที่สุดในเอเชีย โดยอันดับ 2 คือ ฟิลิปปินส์ จำนวน 19.3 ข้อความ และฮ่องกง จำนวน 16.2 ข้อความ แนวโน้มดังกล่าวแสดงให้เห็นว่าปัญหานี้ กำลังเพิ่มขึ้นในภูมิภาค ทำให้ เจ้าหน้าที่และผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ พยายามเตือนให้ ประชาชนเพิ่มความระมัดระวัง เพื่อป้องกันการหลอกลวงและความเสี่ยง ที่อาจทำให้สูญเสียเงิน

# มารู้จักจัดการความเป็นส่วนตัว ก่อนต้องใช้คำว่า รู้จัง... !

## การจัดการความเป็นส่วนตัวในโลกดิจิทัล

### 1 ไม่เผยแพร่ข้อมูลส่วนตัว

ที่มีความสำคัญกับตัวเราให้เป็นสาธารณะ



### 2 จำกัดการเข้าถึงหรือการมองเห็นข้อความ

เพื่อลดโอกาสการเข้าถึงข้อมูลของคนที่ไม่ประสงค์ร้าย



### 3 จัดการอุปกรณ์ให้มีความปลอดภัย

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



#### 4 คิดและอ่าน ก่อนกดตกลงหรือยินยอม

ทำความเข้าใจเงื่อนไขหรือข้อตกลงที่แอปพลิเคชันหรือโปรแกรมร้องขอเข้าถึงข้อมูลส่วนตัว หากอ่านแบบผ่านแล้วกดยอมรับไป ข้อมูลส่วนตัวของเราอาจถูกนำไปใช้ตักตวงผลประโยชน์และถูกละเมิดได้โดยไม่รู้ตัว



#### 5 ตั้งรหัสผ่านให้มีความปลอดภัย

ไม่ใช่รหัสเดียวกันทุกบัญชีในทุกแพลตฟอร์ม ถ้ารู้สึกสงสัยว่า ถูกแฮกให้เปลี่ยนรหัสผ่านใหม่ทันที และหากกังวลว่าจะจำไม่ได้ สามารถใช้ฟังก์ชัน “ลืมหรหัสผ่าน” ได้ นอกจากนี้ ในขณะนี้บางหน่วยงานเริ่มมีการนำมาตรฐานเทคโนโลยีใหม่ มาใช้แทนรหัสผ่านเรียกว่า Passkey ซึ่งจะช่วยให้เราไม่ต้องยุ่งยากกับการจดจำรหัสผ่าน และยิ่งปลอดภัยยิ่งขึ้นอีกด้วย

(ติดตามได้ในด้านที่ 3 Digital Security เรื่องออนไลน์อย่างไรให้ปลอดภัย)



## การจัดการข้อมูลส่วนตัวสำหรับผู้ให้บริการ

ในส่วนของผู้ให้บริการก็ต้องมีมาตรฐานในการจัดการข้อมูลส่วนตัวของเราด้วยเช่นกัน 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 เมื่อต้องเลือกส่งมอบข้อมูลส่วนตัวอันมีค่า ไว้ในการดูแลของผู้ใด และขณะเดียวกัน ผู้ให้บริการนั้น ก็จะต้องมีระบบการพิสูจน์และยืนยันตัวตนที่เข้มแข็งรัดกุมด้วย

**TIP**

โดยระบบยืนยันตัวตนที่ได้รับความนิยม และมีความปลอดภัย มี 2 ระบบด้วยกัน คือ KYC และ E-KYC

## **KYC กระบวนการทำความรู้จักบนโลกดิจิทัล หรือ Know Your Customer แปลตรงตัวว่า "ทำความรู้จักลูกค้าของคุณ"**

แต่ในทางดิจิทัล จะหมายถึง กระบวนการระบุตัวตน - พิสูจน์ตัวตน - ยืนยันตัวตน ของลูกค้าได้อย่างถูกต้อง ซึ่งถือเป็นหลักเกณฑ์สำคัญหนึ่งของ พ.ร.บ. ป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ที่กำหนดให้เป็นหน้าที่ของหน่วยงาน เช่น ธนาคารผู้ให้บริการ e-Wallet e-Payment บริษัทซื้อขายหลักทรัพย์ บริษัทประกัน หรือเรียกว่าเป็นกระบวนการที่จะทำให้ผู้ให้บริการมั่นใจได้ว่า ผู้ที่กำลังติดต่ออยู่นั้น คือ บุคคลนั้นจริง ๆ นั่นเอง

## **E-KYC ย่อมาจากคำว่า "Electronic Know Your Customer" หรือเรียกสั้น ๆ ว่า "E-KYC"**

คือกระบวนการที่ใช้เทคโนโลยีดิจิทัลในการยืนยันและตรวจสอบความถูกต้องของข้อมูล และตัวตนของลูกค้าในรูปแบบอิเล็กทรอนิกส์ ซึ่งใช้ประโยชน์ในการตรวจสอบและยืนยันตัวตนของลูกค้าอย่างรวดเร็วและปลอดภัยยิ่งขึ้น

โดยรูปแบบ E-KYC มักใช้ในรูปออนไลน์ หรือแอปพลิเคชันที่ผู้ใช้บริการสามารถกรอกข้อมูลส่วนตัว และเอกสารประจำตัวอย่างบัตรประชาชน หรือหลักฐานอื่น ๆ และส่งข้อมูลเหล่านั้นไปยังผู้ให้บริการ หรือหน่วยงานที่ต้องการใช้งานได้เลย

ซึ่งในความเป็นจริงแล้ว เมื่อเราติดต่อสื่อสารกับใครบนโลกดิจิทัล หรือผ่านอุปกรณ์สื่อสาร เราก็ควรมีการพิสูจน์และยืนยันตัวตนบุคคลเหล่านั้น ให้แน่ใจก่อนเสมอ เพื่อไม่ให้ตกเป็นเหยื่อผู้ที่สวมรอย อย่างน้อยเมื่อเราต้องกรอกข้อมูลส่วนตัว ข้อมูลทางการเงิน หรือต้องมีการโอนเงิน หรือดาวน์โหลดแอปฯ ใด ๆ มาติดตั้ง



# 5 ทริค

## เสริมเกราะป้องกันภัยคุกคามความเป็นส่วนตัว

1



### ปกป้องอุปกรณ์ของตัวเอง

เช่น ตั้งค่าความเป็นส่วนตัว ไม่กดยินยอมอนุญาตโดยไม่อ่านและไตร่ตรองก่อน สร้างรหัสผ่านที่รัดกุม อัปเดตระบบปฏิบัติการในอุปกรณ์ให้มีความทันสมัยอยู่เสมอ

2



### หมั่นอัปเดตกลโกงที่เกิดขึ้นผ่านช่องทางต่าง ๆ

ทั้งออนไลน์และออฟไลน์ หากเกิดขึ้นกับตัวเองต้องมีสติ และรู้เท่าทัน รวมถึงการมีแหล่งข้อมูล เพื่อการแจ้งกรณีพบเหตุการณ์ไม่พึงประสงค์ทางออนไลน์ ซึ่งอาจจะส่งผลกระทบต่อตัวเราเองและผู้อื่น

3



### คิดให้ดีก่อนโพสต์หรือตอบกลับข้อความ

ตระหนักเสมอว่าสิ่งที่เราโพสต์ไม่สามารถลบออกจากอินเทอร์เน็ตได้อย่างสมบูรณ์

4



### เมื่อต้องซื้อสินค้าหรือบริการผ่านทางออนไลน์

ควรเลือกใช้ช่องทางที่น่าเชื่อถือ และสามารถติดตามถามหาความรับผิดชอบในภายหลังได้

5



### ระวังการบันทึกข้อมูลทางการเงินบนเว็บไซต์ที่ไม่รู้จัก

เพราะอาจเสี่ยงถูกขโมยข้อมูล เช่น เลขที่บัญชีธนาคาร หมายเลขบัตรเครดิต ไปใช้ในทางที่ผิดได้

## EXAMPLE

ยกตัวอย่าง



# ช่องทางติดตามข่าวสาร และแจ้งเหตุ



## ศูนย์รับแจ้งความออนไลน์อาชญากรรมทางเทคโนโลยี


ผ่าน  [www.thaipoliceonline.co.th](http://www.thaipoliceonline.co.th) และ  ศูนย์ AOC 1441


## สำนักงานคณะกรรมการคุ้มครองผู้บริโภค (สคบ.)


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

## ศูนย์ช่วยเหลือและจัดการปัญหาออนไลน์ หรือ 1212 ETDA


รับเรื่องร้องเรียนให้แก่ผู้บริโภคหรือผู้ประกอบการทั้งภาครัฐ และ เอกชน ทั้งในเรื่องเว็บไซต์ผิดกฎหมาย ปัญหาซื้อขายออนไลน์ ปัญหาภัยคุกคามไซเบอร์ และแจ้งปัญหาอื่น ๆ โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หรือ สฟทอ. (ETDA) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

 1212 (24 ชั่วโมง)

 1212@mdes.go.th

 [www.1212ETDA.com](http://www.1212ETDA.com)

 [facebook.com/1212ETDA](https://facebook.com/1212ETDA)

 @1212etda

## ศูนย์ชัวร์ก่อนแชร์ สำนักข่าวไทย อสมท

หน่วยงานด้านการเสริมสร้างความรู้เท่าทัน ตรวจสอบข้อเท็จจริงเรื่องที่แชร์กันบนโซเชียล

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



# กฎหมายที่น่าสนใจ และควรรู้ไว้



## พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ กฎหมาย PDPA

### ย่อมาจาก Personal Data Protection Act

คือ กฎหมายที่กำหนดให้องค์กรหรือหน่วยงานที่จัดเก็บและจัดการข้อมูลส่วนบุคคลของประชาชน ไม่ว่าจะรัฐหรือเอกชน จะต้องได้รับความยินยอมในการเข้าถึง จัดเก็บ จัดการ และคุ้มครองดูแลข้อมูลเหล่านั้น และไม่นำไปใช้ในกิจกรรมที่เราไม่ยินยอม



### 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

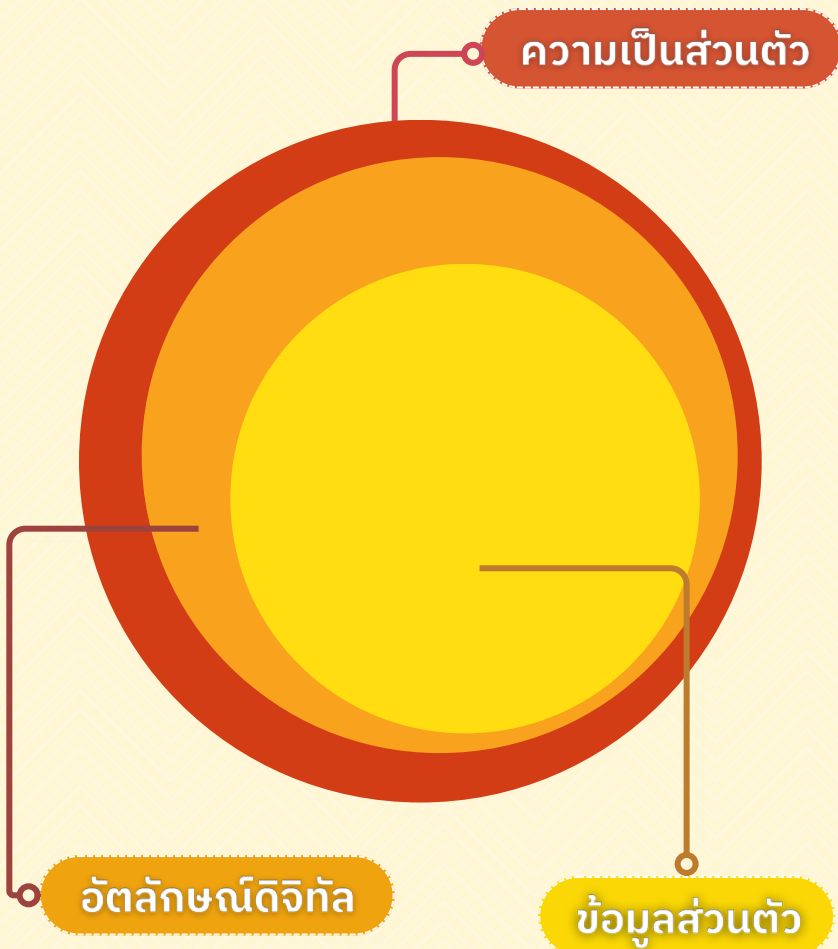
ประวัติอาชญากรรม

ข้อมูลทางด้านสุขภาพ

ข้อมูลชีวภาพ

# ความสัมพันธ์ระหว่าง

อัตลักษณ์ ความเป็นส่วนตัว และข้อมูลส่วนตัว







เราทุกคนล้วนมีเขตหวงห้าม  
 เสมือนความเป็นส่วนตัวต้องรักษา  
 เพราะข้อมูลส่วนตัวบอกชี้ว่า  
 ที่ไม่น่าเผยแพร่ควรเก็บงำ  
 ทั้งชื่อแซ่เลขบัตรแลวันเกิด  
 ถ้าไปเปิดอาจเตลิดโดนรุกร้า  
 เสียชื่อเสียงเสียทรัพย์สุทธระกำ  
 จะไม่ซ้ำถ้าปกป้องไว้ให้ดี

เพราะทุกคน  
ล้วนมีโลกอีกใบ

กิจกรรมต่าง ๆ  
ในโลกดิจิทัล

ติดต่อสื่อสาร

ใช้บริการหน่วยงาน  
ภาครัฐและเอกชน

แบ่งปันข้อมูลข่าวสาร

ทำธุรกรรมทางการเงิน

**Biometrics**

สิ่งที่ใช้แยกแยะตัวตน  
ของแต่ละบุคคล

ลักษณะทางสรีรวิทยา

ลักษณะเฉพาะทาง  
พฤติกรรม

ผลจากการสร้าง  
อัตลักษณ์ทางดิจิทัล

ผลลัพธ์สุดว้าว

ผลกระทบสทบหวง

## 1.1

## Digital Citizen Identity

รู้ได้อย่างไร  
ใครเป็น  
เจ้าของอัตลักษณ์ ?

การระบุตัวตน  
(Identification)

การพิสูจน์ตัวตน  
(Identity Proofing)

การยืนยันตัวตน  
(Authentication)

อะไรคือ สิ่ง  
ที่แสดงตัวตน  
ของเราในโลกดิจิทัล ?

3 องค์ประกอบหลัก  
ปึกหมุดอัตลักษณ์ดิจิทัล

Personal  
Information (PII)

Social & Behavioral  
Information

Digital  
Information

**การดูแล  
อัตลักษณ์ดิจิทัล**

How to 3 STEP  
ในการปรับปรุงอัตลักษณ์ดิจิทัล

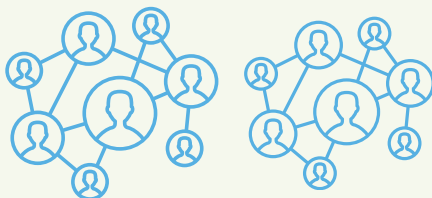
คาถา 8 ข้อ เสริมชีวิต  
สร้างอัตลักษณ์ดิจิทัลที่ดี

แนวปฏิบัติที่ดีในการจัดการ  
อัตลักษณ์ดิจิทัล





02



การใช้เทคโนโลยีดิจิทัล  
อย่างเหมาะสม

— Digital Use —

# แนะนำสำหรับผู้สอน



## • วัตถุประสงค์

ผู้เรียนมีความรู้เกี่ยวกับการค้นหา รวบรวม และจัดการข้อมูลที่ต้องการจากสื่อดิจิทัล อธิบายถึงการแบ่งเวลาสำหรับการใช้เทคโนโลยีที่เหมาะสมและผลกระทบที่เกิดขึ้นได้

## • ขอบเขตของเนื้อหาเรื่องนี้

2.1 Balanced Use of Technology การใช้เทคโนโลยีอย่างมีความสมดุล



การดูแลสุขภาพบนโลกดิจิทัล (Digital Health)

วันที่สอน  
/././.



การบริหารจัดการเวลาบนโลกดิจิทัล (Screen Time

Management)

วันที่สอน  
/././.






การมีส่วนร่วมอย่างสร้างสรรค์ในชุมชนดิจิทัล

วันที่สอน  
/././.

## • ขอบเขตของเนื้อหาเรื่องนี้

### 2.2 Civic Use of Technology การใช้เทคโนโลยี เพื่อสังคมและตนเอง

-  การใช้เทคโนโลยีในโลกดิจิทัลเพื่อสังคมและตนเอง วันที่สอน  
/././
-  การใช้เทคโนโลยีอย่างเหมาะสมเพื่อสร้างค่านิยมเชิงบวกต่อชุมชน  
และพัฒนาคุณภาพชีวิต วันที่สอน  
/././
-  การสืบค้นข้อมูลจากสื่อดิจิทัล วันที่สอน  
/././

เวลาในการเรียน



# รู้ศัพท์

## ไม่ลับสน



1



### ERGONOMICS

คือ วิทยาการเพื่อการทำงาน โดยใช้วิทยาศาสตร์  
เชื่อมโยงสัมพันธ์กับเนื้องาน บุคลากร  
สภาพแวดล้อม เพื่อออกแบบลักษณะ  
ของการทำงานให้มีประสิทธิภาพ  
ลดความเสี่ยงผลกระทบต่อสุขภาพหรืออันตรายจากอุบัติเหตุ

2



### DIGITAL HEALTH

คือ การดูแลสุขภาพและความเป็นอยู่ที่ดี  
ในยุคดิจิทัล โดยมุ่งเน้นการใช้เทคโนโลยี  
อย่างเหมาะสมและสมดุล เพื่อส่งเสริมสุขภาพ  
ทั้งทางร่างกาย จิตใจ และการดำเนินชีวิตโดยรวม

3



### PHYSICAL HEALTH

คือ สภาวะความสมบูรณ์ของร่างกาย

4



### MENTAL HEALTH

คือ สภาวะความสมดุลของจิตใจ อารมณ์ สังคม  
และจิตวิญญาณ ซึ่งมีผลต่อการตัดสินใจ  
หรือ แก้ปัญหาต่าง ๆ

# รู้ศัพท์

# ไม่ลับสน



5



## SCREEN TIME

คือ คำที่ใช้เรียกกิจกรรมต่าง ๆ บนหน้าจอดิจิทัล

6



## CONTENT ADDICTION

### หรือ การเสพติดเนื้อหา

คือ เป็นภาวะติดการเสพข้อมูลหรือเนื้อหาบนสื่อดิจิทัล ทำให้เกิดผลกระทบต่อการทำงาน การเรียน และการขาดปฏิสัมพันธ์กับคนรอบข้างอย่างเห็นได้ชัด

7



## DIGITAL WELLBEING

### หรือ สุขภาวะดิจิทัล

คือ การใช้เทคโนโลยีดิจิทัลในเชิงบวก เพื่อส่งเสริมสุขภาพกาย สุขภาพจิต และความเป็นอยู่ที่ดี โดยไม่ให้ส่งผลเสียต่อชีวิตประจำวันและมีสุขภาพที่ดี



หากคุณเรียนผ่านด้านนี้  
คุณจะไม่เสี่ยงเป็น  
โรคออฟฟิศซินโดรม  
รวมถึงโรคติดจอได้

# 2.1

## BALANCED USE OF TECHNOLOGY

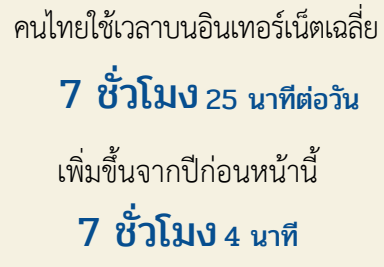
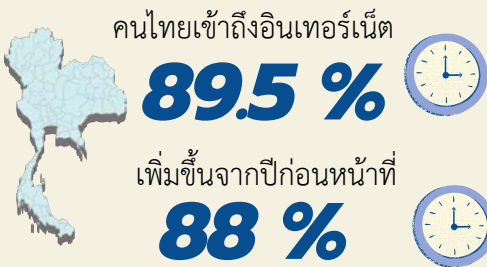
### วัตถุประสงค์

1. ผู้เรียนอธิบายถึงการแบ่งเวลา ในการใช้เทคโนโลยีโดยคำนึงถึงผลกระทบต่อสุขภาพ การทำงาน สุขภาวะ การดำเนินชีวิตประจำวันได้
2. ผู้เรียนสามารถเลือกและใช้เครื่องมือหรืออุปกรณ์หรือเทคโนโลยีที่ส่งผลดีต่อสุขภาพ (ERGONOMICS) ได้
3. ผู้เรียนสามารถเข้าใจถึงการจัดการ และตั้งค่าการเข้าถึงเนื้อหา ที่เหมาะสม เพื่อป้องกันการเสพติดเนื้อหาที่มีผลกระทบต่อสุขภาพจิตของตนเอง

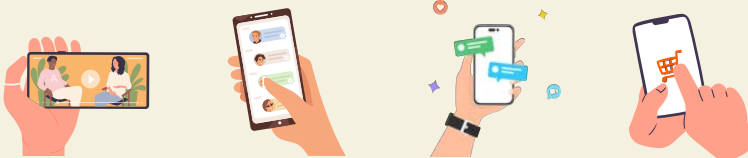


เทคโนโลยีพัฒนาอย่างรวดเร็ว ส่งผลให้พฤติกรรมการใช้เทคโนโลยีของคนไทยมีแนวโน้มเปลี่ยนแปลงไปอย่างต่อเนื่อง โดยเทคโนโลยีดิจิทัลเข้ามามีบทบาทสำคัญในชีวิตประจำวันของคนไทยมากขึ้น ไม่ว่าจะเป็นการใช้เพื่อการสื่อสาร การทำงาน การเรียน การศึกษาหาความรู้ และความบันเทิง

จากผลสำรวจพฤติกรรมการใช้อินเทอร์เน็ตของคนไทยในปี 2566 โดยสำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) พบว่า



กิจกรรมที่คนไทยนิยมทำบนอินเทอร์เน็ต ได้แก่ รับชมวิดีโอคอนเทนต์ พุดคุยบนบล็อกและกระทู้ โอนเงินผ่านเว็บไซต์ ช้อปปิ้งออนไลน์ และสื่อความบันเทิงในโลกออนไลน์



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 จำเป็นต้องมีการจัดการในหลากหลายด้าน แบ่งออกเป็น 3 กลุ่มใหญ่ ๆ ประกอบด้วย

### 1 การดูแลสุขภาพบนโลกดิจิทัล (Digital Health)

ปกป้องสุขภาพกายและสุขภาพจิตในการใช้งานโลกดิจิทัล



### 2 การบริหารจัดการเวลาหน้าจอ (Screen Time Management)

จัดสรรเวลาในการใช้งานอุปกรณ์และสื่อดิจิทัลได้อย่างสมดุล



### 3 การมีส่วนร่วมอย่างสร้างสรรค์ในชุมชนดิจิทัล

ร่วมเสริมสร้างชุมชนดิจิทัลที่ดี และหลีกเลี่ยงผลกระทบเชิงลบ



# การดูแลสุขภาพ บนโลกดิจิทัล (Digital Health)



เทคโนโลยีสามารถส่งผลกระทบต่อสุขภาพกายและสุขภาพจิตของเรา โดยหากเราใช้งานอย่างไม่สมดุล ย่อมส่งผลกระทบต่อสุขภาพทุกด้าน ดังนั้น การรักษาสุขภาพดิจิทัลที่ดีจึงมีความสำคัญ เพื่อให้เราสามารถได้ประโยชน์จากเทคโนโลยีได้อย่างเต็มที่โดยไม่กระทบต่อสุขภาพของเรา

สุขภาพดิจิทัล (Digital Health) คือ การดูแลสุขภาพและความเป็นอยู่ที่ดีในยุคดิจิทัล โดยมุ่งเน้นการใช้เทคโนโลยีอย่างเหมาะสมและสมดุล เพื่อส่งเสริมสุขภาพ ทั้งทางร่างกาย จิตใจ และการดำเนินชีวิตโดยรวม

การดูแลสุขภาพบนโลกดิจิทัล แบ่งเป็น 2 ด้าน คือ การดูแลสุขภาพกาย และการดูแลสุขภาพจิต

## สุขภาพกาย (Physical Health)

ในการใช้งานดิจิทัลไม่ว่าผ่านอุปกรณ์ในรูปแบบใด ล้วนเกี่ยวข้องกับการใช้งานร่างกายแทบทั้งสิ้น ดังนั้น การใช้งานที่ผิดวิธีหรือมากเกินไป จึงส่งผลโดยตรงต่อร่างกายอย่างหลีกเลี่ยงไม่ได้

### 1.1. ดวงตา



การมองภาพจากหน้าจออย่างไม่เหมาะสม อาจส่งผลให้มีอาการตาแห้ง แสบตา ปวดตา ตาพร่ามัว และอาจส่งผลต่อการมองเห็นในระยะยาวได้



### วิธีดูแลสุขภาพตา :

- ใช้หลัก **20-20-20** คือ พักสายตาเป็นประจำทุก 20 นาที โดยละสายตาจากหน้าจอและมองไปยังวัตถุที่อยู่ไกลออกไปประมาณ 20 ฟุต เป็นเวลา 20 วินาที
- ปรับความสว่างหน้าจอให้อยู่ในระดับที่เหมาะสม ไม่สว่างหรือมืดเกินไป
- ใช้แสงไฟที่เหมาะสมในขณะที่ใช้งานหน้าจอ หลีกเลี่ยงการใช้หน้าจอในที่มืด
- ตรวจสุขภาพตากับจักษุแพทย์เป็นประจำ

## 1.2. หู

โดยเฉพาะผู้ที่มักใช้หูฟัง การฟังเสียงในระดับที่ดังเกินไปเป็นเวลานานส่งผลกระทบท่อหู และอาจทำให้สูญเสียการได้ยิน

### วิธีดูแลสุขภาพหู :

- ปรับระดับเสียงให้เหมาะสม ไม่ดังเกินไป
- จำกัดเวลาในการใช้หูฟัง
- หากรู้สึกว่ามีหูอื้อหรือมีเสียงดังในหู ควรหยุดใช้หูฟังและปรึกษาแพทย์

### 1.3 ร่างกาย



การจัดตำแหน่งร่างกายในอิริยาบถต่าง ๆ หรือการขยับท่าทางแบบผิดวิธี อาจส่งผลให้เกิดอาการปวดหลัง 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 ยังส่งผลกระทบต่ออีกด้านหนึ่ง นั่นคือ การนอนที่ไม่มีคุณภาพนอนหลับไม่สนิทหรือยิ่งกว่านั้น คือ การนอนไม่เพียงพอ หรือนอนไม่หลับ การโหมทำงาน โหมดูภาพยนตร์ โหมเสพเนื้อหาความบันเทิง อาจเป็นสาเหตุหลักของการนอนที่ไม่มีคุณภาพ

อีกหนึ่งปัจจัยสำคัญที่ส่งผลกระทบต่อการนอน คือการใช้งานหน้าจอ เพราะ “แสงสีฟ้า” จากหน้าจอจะมารบกวนการผลิตเมลาโทนิน ซึ่งเป็นฮอร์โมนที่ช่วยในการนอนหลับของร่างกาย

## วิธีแก้ไข

- จำกัดเวลาการใช้งานหน้าจอ หยุดใช้งานหน้าจอต่าง ๆ อย่างน้อย 1 - 2 ชั่วโมงก่อนนอน
- สร้างสภาพแวดล้อมการนอนหลับที่เหมาะสม มีด สงบ และอุณหภูมิที่เหมาะสม
- หลีกเลี่ยงการดื่มเครื่องดื่มที่มีกาเฟอีนหรือแอลกอฮอล์ก่อนนอน

## 1.5 สุขภาพโดยรวม

การใช้งานดิจิทัล อาจทำให้หลงลืมการดูแลสุขภาพโดยรวม อีกทั้งโดยส่วนใหญ่เรามักใช้งานโดยนั่งอยู่กับที่ (และอาจมีน้ำหวาน หรือขนมติดมือติดโต๊ะไม้ขาด) จึงเสี่ยงไม่ได้ที่จะเกิด “สภาวะเนือยนิ่ง” และอาจนำมาซึ่งโรคภัยไข้เจ็บ โรคไม่ติดต่อเรื้อรัง อย่างโรคเบาหวาน โรคอ้วน โรคหัวใจและหลอดเลือด โรคทางระบบประสาท รวมถึงปัญหาสุขภาพอื่น ๆ ตามมาได้

## วิธีแก้ไข

- ให้ความสำคัญกับการใช้ชีวิตนอกจอ ขยับร่างกายลุกขึ้นยืน และเดินให้มากเท่าที่จะทำได้
- ดูแลอาหารการกิน หากจำเป็นต้องมีอาหารว่าง ควรเลือกอาหารที่ไม่ส่งผลเสียต่อสุขภาพ เครื่องดื่มควรเน้นน้ำเปล่า หรือเครื่องดื่มที่ไม่มีน้ำตาลมากเกินไป
- จัดสรรเวลาออกกำลังกาย อย่างน้อย 30 นาทีต่อวัน 5 วันต่อสัปดาห์ โดยมองหากิจกรรมที่คุณชอบทำ เช่น เดิน วิ่ง ว่ายน้ำ หรือเล่นกีฬา
- ใช้เทคโนโลยีเพื่อช่วยติดตามและสร้างแรงบันดาลใจในการทำกิจกรรมหรือออกกำลังกาย เช่น แอปพลิเคชันนับก้าว สมาร์ทวอตช์ เป็นต้น



## รู้จักหลัก

# "การยศาสตร์" หรือ Ergonomics เคล็ดลับป้องกันผลกระทบต่อสุขภาพ

### การยศาสตร์ (Ergonomics) คือ

วิทยาการเพื่อการทำงาน โดยใช้วิทยาศาสตร์เชื่อมโยงสัมพันธ์กับเนื้องาน บุคลากร สภาพแวดล้อม เพื่อออกแบบลักษณะของการทำงานให้มีประสิทธิภาพ ลดความเสี่ยง ผลกระทบต่อสุขภาพหรืออันตรายจากอุบัติเหตุ

1



#### ไม่ไหวอย่าฝืน

ใช้ร่างกายเป็นมาตรฐาน  
เมื่อร่างกายเริ่มมีอาการผิดปกติ  
ก็ควรหยุดพักจากการใช้งานก่อน

2



#### กฎ 20-20-20

พักสายตาเป็นประจำทุก 20 นาที  
โดยละสายตาจากหน้าจอ และมองไปยังวัตถุ  
ที่อยู่ไกลออกไปประมาณ 20 ฟุต  
เป็นเวลา 20 วินาที

3



#### นั่งท่าที่สบาย

ระหว่างที่อยู่หน้าจควรจัดโต๊ะเก้าอี้  
ให้นั่งอยู่ในท่าที่ถูกต้อง  
ไม่สร้างการบาดเจ็บต่อร่างกาย  
ปรับแสงหน้าจอให้อยู่ในระดับพอดี

4



#### ตั้งเป้าหมายการใช้งาน

ตั้งเป้าหมายก่อนการใช้งาน  
หน้าจอทุกครั้ง  
และควรจำกัดเวลาการอยู่หน้าจอ

5



#### ทำกิจกรรมอื่นบ้าง

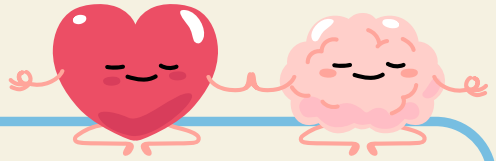
หากิจกรรมอย่างอื่นทำ ที่ไม่ต้องอยู่หน้าจอ  
ตลอดเวลา เช่น ออกกำลังกายอย่างน้อย  
30 นาทีต่อวัน หรือออกไปท่องเที่ยว

6



#### พักผ่อนให้เพียงพอ

รับประทานอาหารที่มีประโยชน์  
นอนหลับพักผ่อนให้เพียงพอ  
อย่างน้อย 6 - 8 ชั่วโมงต่อคืน



## สุขภาพจิต (Mental Health)

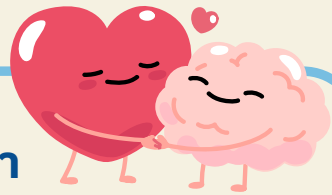
ในการใช้งานดิจิทัลนอกจากร่างกายที่มีปฏิสัมพันธ์กับอุปกรณ์ต่าง ๆ แล้ว ในขณะเดียวกันจิตใจและความรู้สึกนึกคิด ก็มีส่วนปฏิสัมพันธ์โดยตรงกับเนื้อหา ข้อมูลข่าวสาร และการตอบสนองต่อเหตุการณ์ทางดิจิทัลที่เกิดขึ้นด้วย

### 2.1 จัดการอารมณ์ และความรู้สึก

การเสพเนื้อหา ข่าวสาร หรือพบเจอเหตุการณ์ที่มีความรุนแรง สะเทือนอารมณ์ และความรู้สึกก็อาจส่งผลทำให้เกิดความเครียด ความวิตกกังวล จนกลายเป็นโรคซึมเศร้าได้

#### วิธีแก้ไข

- จำกัดการรับข่าวสารและข้อมูลที่มีมากเกินไป เลือกติดตามข่าวสารจากแหล่งที่เชื่อถือได้ และจำกัดเวลาในการเสพข่าวสาร
- การหมั่นฝึกสติและสมาธิ ช่วยให้เราีสติอยู่กับปัจจุบัน และลดความฟุ้งซ่านในจิตใจได้
- หากิจกรรมที่ช่วยผ่อนคลายความเครียดทำ เช่น การฟังเพลง การอ่านหนังสือ การออกกำลังกาย หรือการทำกิจกรรมที่ชอบ
- พูดคุยกับเพื่อนหรือคนในครอบครัว แบ่งปันความรู้สึก กับคนใกล้ชิด จะช่วยลดความเครียด และความวิตกกังวลได้



## 2.2 ใส่ใจความสัมพันธ์ที่มีคุณค่า

การใช้เวลากับเนื้อหา และเทคโนโลยีมากเกินไป จนละเลยความสัมพันธ์กับคนรอบข้าง อาจทำให้รู้สึกโดดเดี่ยว และมีปัญหาในการปฏิสัมพันธ์กับคนจริง ๆ ได้

### วิธีแก้ไข

- จัดสรรเวลาพบปะพูดคุยกับเพื่อนและครอบครัวเป็นประจำ การมีปฏิสัมพันธ์กับคนรอบข้าง จะช่วยให้เราไม่รู้สึกโดดเดี่ยว
- เข้าร่วมกิจกรรมทางสังคม การเข้าร่วมกิจกรรม ช่วยให้เราได้พบปะผู้คนใหม่ ๆ และสร้างความสัมพันธ์ที่ดีต่อกันได้
- ใช้เทคโนโลยีเพื่อเชื่อมต่อกับคนที่เรารัก การติดต่อสื่อสารกับคนที่เรารัก จะช่วยให้เรารู้สึกใกล้ชิดและได้รับการสนับสนุนอยู่เสมอ
- หลีกเลี่ยงการเปรียบเทียบตัวเองกับผู้อื่นบนโซเชียลมีเดีย เพราะอาจทำให้เกิดความรู้สึกไม่พอใจในตนเองและลดทอนความมั่นใจ

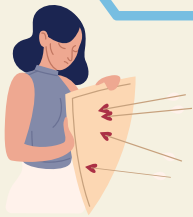


## 2.3 รู้ทันพฤติกรรมการใช้เทคโนโลยี

การใช้เทคโนโลยีมากเกินไป อาจทำให้เกิดพฤติกรรมที่ส่งผลเสียต่อจิตใจ ลุกกลามไปจนถึงการเสพติด หรือก่อให้เกิดภาวะซึมเศร้า ซึ่งไม่จำกัดอยู่แค่ในโลกดิจิทัล แต่แสดงผลในโลกความเป็นจริง

### วิธีแก้ไข

- หมั่นสังเกตความผิดปกติทางจิตใจและพฤติกรรมของตนเอง รู้เท่าทันความรู้สึกนึกคิด ไม่ปล่อยให้สิ้นหวังกับตนเอง เพียงเพราะสิ่งที่พบในโลกดิจิทัล
- ศึกษาข้อมูลเกี่ยวกับสุขภาพจิตจากแหล่งที่น่าเชื่อถือ เพื่อให้มีความรู้ความเข้าใจเกี่ยวกับสุขภาพจิต และวิธีการดูแลตนเอง
- ใช้แอปพลิเคชัน หรือเครื่องมือออนไลน์ ที่ช่วยในการดูแลสุขภาพจิต เช่น แบบทดสอบสุขภาพจิต เป็นต้น
- หากสงสัยว่ามีปัญหาสุขภาพจิต ควรปรึกษาผู้เชี่ยวชาญ นักจิตวิทยา หรือจิตแพทย์ เพื่อเข้ารับการช่วยเหลือ หรือคำแนะนำในการจัดการปัญหาสุขภาพจิตได้อย่างมีประสิทธิภาพ



## แนวทางป้องกันสุขภาพจิต จากผลกระทบด้านลบ

มีวิธีง่าย ๆ ดังต่อไปนี้

### 1 กำหนดระยะเวลาที่ใช้ในการเสพเนื้อหา



แบ่งเวลาที่ใช้เสพเนื้อหา เวลาพักผ่อนอย่างเหมาะสม เพื่อให้ไม่  
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



## Digital Fatigue

### หรือ “การเหนื่อยล้าจากการใช้งานดิจิทัล”

คือ ภาวะที่เกิดขึ้นเมื่อเรารู้สึกเหนื่อยหรือล้าจากการใช้งาน และการเชื่อมต่อกับเทคโนโลยีดิจิทัลอย่างต่อเนื่องหรือในปริมาณมาก โดยมักเกิดขึ้นเมื่อมีการใช้งานอุปกรณ์ดิจิทัล โปรแกรมคอมพิวเตอร์ และแพลตฟอร์มออนไลน์เป็นเวลานาน ๆ โดยไม่มีการพักผ่อน หรือการเปลี่ยนแปลงกิจวัตรประจำวัน

### อาการ Digital Fatigue

คือ มักรู้สึกเหนื่อยล้า มีความสับสน หรือไม่พร้อมที่จะดำเนินกิจวัตรประจำวันต่อไป เพราะการเหนื่อยจากดิจิทัลอาจมีผลกระทบต่อร่างกาย และจิตใจ เช่น ปวดตา ปวดหลัง ภาวะเครียด หรือภาวะซึมเศร้า

### การดูแลและรักษา Digital Fatigue

ควรมีการจัดการเวลาที่ใช้ในโลกดิจิทัล เปลี่ยนแปลงกิจวัตรประจำวัน ให้มีความสำคัญกับการดูแลสุขภาพจิต การใช้เทคโนโลยีอย่างมีสติ และมีความสุข จะสามารถช่วยลดความเหนื่อยล้าที่เกิดขึ้นจากการใช้งานดิจิทัลได้



# การบริหารจัดการ

## เวลาบนโลกดิจิทัล



### 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



# การใช้เวลาน้ำจอดีigital ที่เหมาะสมกับแต่ละช่วงวัย

องค์การอนามัยโลก (WHO) แนะนำว่า

**1** เด็กอายุต่ำกว่า 2 ปี



ควรหลีกเลี่ยงการใช้หน้าจอ

**2** เด็กอายุ 2-5 ปี



ควรใช้เวลาไม่เกิน 1 ชั่วโมง  
ต่อวัน และควรดูเฉพาะ  
สิ่งส่งเสริมพัฒนาการ  
ทางการศึกษา

**3** เด็กอายุ 5 ปีขึ้นไป



ไม่ควรเกิน 2 ชั่วโมงต่อวัน  
และไม่เกิน 3 ชั่วโมงต่อวัน  
ในช่วงสุดสัปดาห์

**4** ผู้ใหญ่



ควรเฉลี่ยแล้วไม่เกิน  
วันละ 2 ชั่วโมง  
จึงจะถือว่าเป็นเวลาที่  
ไม่ก่อให้เกิดอันตรายต่อสุขภาพ



## ต้นเหตุแห่งอาการเสพติดหน้าจอ

### หรือ Screen Addiction

หากเราดำเนินชีวิตโดยใช้เวลามากอยู่กับหน้าจอมากเกินไป ไม่ว่าจะ เป็น หน้าจอ โทรศัพท์ จอคอมพิวเตอร์ จอ Tablet หรือจอมือถือ อาจทำให้เรามีอาการ **เสพติดหน้าจอ หรือ Screen Addiction**

### ภาวะติดจอ (screen addiction)

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

### อาการที่บ่งบอกว่ากำลังเสพติดการใช้หน้าจอ

- 1) รู้สึกหงุดหงิดกระวนกระวาย เมื่อไม่ได้ใช้สื่อออนไลน์
- 2) ให้ความเวลากับสื่อออนไลน์มากเกินไป 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 แลบางคนยังมีขนมหวานและเครื่องดื่มผสมน้ำตาลไม่ขาดมือ ส่งผลให้น้ำหนักเพิ่มขึ้นและเสี่ยงต่อโรคอ้วน โรคเบาหวาน และโรคหัวใจ

04



### ปัญหาด้านนอนหลับ

แสงสีฟ้าจากหน้าจอสามารถรบกวนการหลั่งฮอร์โมนเมลาโทนิน ที่เป็นสารซึ่งช่วยในการนอนหลับ ทำให้นอนหลับยากหรือนอนไม่หลับ

# ผลกระทบจากการเสพติดหน้าจอ

## ผลกระทบต่อการดำเนินชีวิต

01



### ปัญหาด้านความสัมพันธ์

การใช้เวลากับหน้าจอมากเกินไปอาจทำให้เราละเลยความสัมพันธ์กับคนรอบข้าง ขาดปฏิสัมพันธ์กับผู้อื่น และอาจนำไปสู่ปัญหาทางอารมณ์ เช่น ภาวะซึมเศร้า และปัญหาด้านความสัมพันธ์

02



### ปัญหาด้านการทำงาน

การใช้เวลากับหน้าจอที่ไม่ใช่การทำงานมากเกินไป อาจทำให้เราทำงานไม่มีประสิทธิภาพ ความรับผิดชอบลดน้อยลง และอาจพลาดโอกาสในการทำงานได้

03



### ปัญหาด้านการศึกษา

การใช้เวลากับหน้าจอมากเกินไปอาจทำให้เราเสียสมาธิ วอกแวกง่าย เรียนไม่เข้าใจ และอาจส่งผลต่อผลการเรียนได้

04



### ปัญหาด้านการเงิน

การใช้เวลากับหน้าจอ หรือโลกออนไลน์ที่มีสินค้าอยู่ มากมาย ทำให้เราใช้จ่ายมากเกินไป เพราะซื้อสินค้าได้ง่าย และหากเราไม่ดูแลสุขภาพ อาจจำเป็นต้องนำเงินที่หามาได้ไปเป็นค่ารักษาพยาบาล



## ห้ามใจจากจอไม่ได้

### 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

เป็นวิธีที่มีประสิทธิภาพในการจัดการเวลาและเพิ่มความสม่ำเสมอในการทำงาน 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

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

## 5 Focus Apps

แอปพลิเคชันที่ช่วยในการรักษาความมีสมาธิ และไม่ทำให้เสียเวลา เช่น Forest ที่ให้คุณปลูกต้นไม้ขณะที่คุณทำงานและต้องปกป้องต้นไม้จนกว่าจะสำเร็จงาน

## 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

นอกจากบางคนจะเป็นภาวะเสพติดใจแล้ว ก็อาจจะมีอีกอาการที่เรียกว่า การเสพติดเนื้อหา

### การเสพติดเนื้อหา (Content Addiction)

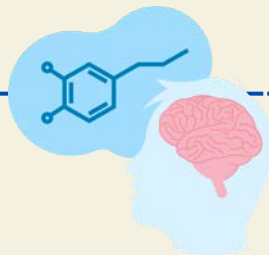
เป็นภาวะติดการเสพข้อมูล หรือเนื้อหาบนสื่อดิจิทัล เช่น โซเชียลมีเดีย เกมออนไลน์ และวิดีโอ

### อาการของการเสพติดเนื้อหา

- ไม่สามารถควบคุมตัวเองได้เมื่อเห็นเนื้อหาที่สนใจ
- ใช้เวลาไปกับเนื้อหามากเกินไปจนกระทบต่อการเรียน การงาน หรือความสัมพันธ์กับคนรอบข้าง
- รู้สึกหงุดหงิดหรือกระวนกระวายเมื่อไม่ได้เสพเนื้อหา

### สาเหตุของการเสพติดเนื้อหา มีดังนี้

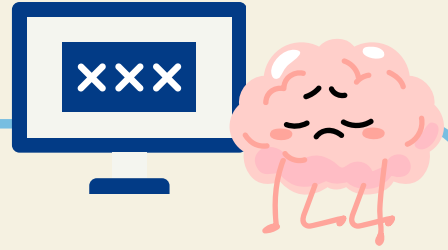
- 1) **ปัจจัยทางชีวภาพ** พบว่าในสมองของผู้เสพติดเนื้อหา มักมีสารโดปามีนในระดับต่ำ ซึ่งสารโดปามีนนี้ ทำหน้าที่ควบคุมอารมณ์ การเรียนรู้ และการเคลื่อนไหว
- 2) **ปัจจัยทางจิตวิทยา** ผู้เสพติดเนื้อหามักมีแนวโน้มที่จะรู้สึกโดดเดี่ยว เหงา หรือขาดความมั่นใจในตัวเอง
- 3) **ปัจจัยทางสังคม** สังคมในปัจจุบันให้ความสำคัญกับเทคโนโลยีเป็นอย่างมาก ผู้คนมักใช้เวลาส่วนใหญ่ไปกับการใช้อุปกรณ์ดิจิทัล ซึ่งอาจกระตุ้นให้เกิดพฤติกรรมเสพติดเนื้อหาได้

**TIP**

## สารโดปามีน (dopamine)

เป็นสารสื่อประสาทที่มีบทบาทสำคัญเรื่องอารมณ์ และความรู้สึก มักถูกเรียกว่าเป็นสาร "รู้สึกดี" เพราะถูกปล่อยออกมาเพื่อตอบสนองต่อประสบการณ์ที่น่าพึงพอใจ และสามารถช่วยยกระดับอารมณ์ได้

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



## การเสพติดเนื้อหา

 มักจะส่งผลให้เกิดผลเสียต่อสุขภาพจิต

### 1 ด้านอารมณ์

การติดตามเนื้อหา หรือข่าวสารที่มีความเครียดสูง นำเสนอแต่ความไม่มั่นคงในชีวิต สามารถทำให้เกิดความเครียดที่ไม่จำเป็น มีความวิตกกังวล หรืออาการซึมเศร้าได้

### 2 ด้านความสัมพันธ์

การที่เราเสพติดเนื้อหาและใช้งานอินเทอร์เน็ตมาก ๆ จนละเลยคนรอบข้าง และในชีวิตจริงกลับทำอะไรรคนเดียว เมื่อเกิดปัญหาขึ้นเราอาจจะไม่มีคนให้ปรึกษา ไม่ไว้วางใจใคร รู้สึกโดดเดี่ยว

### 3 ด้านพฤติกรรม

การใช้เวลาในการเสพติดเนื้อหามากเกินไป อาจทำให้ขาดสมดุลในชีวิต ระหว่างการทำงาน การพักผ่อน และสังคม มีผลต่อสุขภาพจิตที่ดี

นอกจากนี้ อาจนำไปสู่ปัญหาสุขภาพจิตอื่น ๆ เช่น โรควัยาคิดย้ำทำ (OCD) โรควิตกกังวลทางสังคม (SAD) และโรคบุคลิกภาพแบบก้ำกึ่ง (BPD) หากพบว่าตัวเองมีปัญหาเรื่องการเสพติดเนื้อหา ให้ลองปรึกษาผู้เชี่ยวชาญเพื่อขอคำแนะนำ

**TIP****โรคว้าคิดว้าทำ**

(OCD หรือย่อมาจาก Obsessive Compulsive Disorder)

เป็นโรคทางจิตเวชชนิดหนึ่ง ที่ผู้ป่วยจะมีความกังวลหรือความไม่มั่นใจต่อสิ่งใดสิ่งหนึ่ง จึงพยายามแก้ไขด้วยการทำกิจกรรมบางอย่างซ้ำไปซ้ำมา

**โรควิตกกังวลทางสังคม**

(SAD หรือย่อมาจาก Social anxiety disorder)

การที่ผู้ป่วยมีอาการประหม่า รู้สึกไม่สบายใจ อึดอัด กังวลใจ เมื่ออยู่ในสถานการณ์ที่อาจมีผู้อื่นสังเกตจ้องมองตนเองอยู่

**โรคบุคลิกภาพแบบก้ำกึ่ง**

(BPD หรือย่อมาจาก Borderline Personality Disorder)

เป็นความผิดปกติทางจิต ที่ส่งผลต่อความคิดและความรู้สึกที่ผู้ป่วยมีต่อตนเองและผู้อื่น ผู้ป่วยอาจมีอาการรุนแรงขึ้น ๆ ลง ๆ อารมณ์รุนแรง หุนหันพลันแล่น มีความคิดและนิสัยไม่คงที่ ซึ่งส่งผลให้มีปัญหาในการรักษาความสัมพันธ์กับผู้อื่น และการใช้ชีวิตประจำวัน

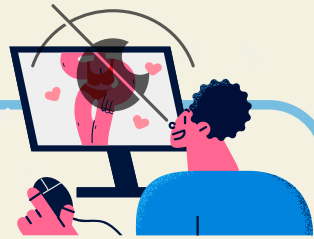


## ติดจอนต่อต้านสังคม

คนที่ติดจอนมากเกินไป อาจมีพฤติกรรมต่อต้านสังคม อันเนื่องมาจากการเสพเนื้อหาที่มีความรุนแรง หรือขัดแย้งอย่างต่อเนื่อง ทำให้มีความเห็นที่สุดโต่ง มีการแสดงออกที่ก้าวร้าว ด่าทอผู้อื่นโดยไม่รู้ตัว

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





## ลักษณะเนื้อหาที่เราควรพิจารณา เพื่อป้องกันการเสพติดเนื้อหาที่ไม่เหมาะสม

- 1 มีความถูกต้องแม่นยำ ไม่บิดเบือนหรือจงใจใส่ข้อมูลเท็จ
- 2 ความเป็นปัจจุบัน ทันสมัยและทันต่อเหตุการณ์
- 3 กระชับ ชัดเจน เข้าใจง่าย และตรงประเด็น
- 4 มีความเหมาะสมกับกลุ่มเป้าหมายที่ตั้งใจจะสื่อสาร
- 5 สร้างสรรค์ น่าสนใจและเป็นประโยชน์ต่อผู้อื่น
- 6 ไม่มีเนื้อหาที่ก่อให้เกิดความขัดแย้ง ความรุนแรง และอคติ
- 7 หลีกเลี่ยงเนื้อหาที่ไม่เหมาะสมกับศีลธรรม จริยธรรม
- 8 ไม่มีเนื้อหาละเมิดลิขสิทธิ์
- 9 ไม่มีภาพหรือเนื้อหาเชิงล่อเลียน ขบขัน หรือภาพแอบถ่ายโดย  
ไม่ได้รับอนุญาต

## การจัดการ และตั้งค่าการเข้าถึงเนื้อหาบนแพลตฟอร์มต่าง ๆ เพื่อป้องกันการเสพติดเนื้อหา

### ตั้งค่าการกรองเนื้อหาแพลตฟอร์มต่าง ๆ

ตั้งค่าให้กรองเนื้อหาตามคำหลักที่เราต้องการบนโซเชียลมีเดียอย่าง แพลตฟอร์ม X (Twitter) ตรงหัวข้อ ความเป็นส่วนตัว และความปลอดภัย ด้วยการกำหนดคำเพื่อซ่อนและบล็อกคำที่ต้องการ เช่น ฆ่าตัวตาย การทำร้ายร่างกาย ยาเสพติด



### จำกัดระยะเวลาในอ่านหรือเข้าชมเนื้อหา

ของแอปพลิเคชันต่าง ๆ ด้วย Digital wellbeing เช่น การตั้งค่าการจำกัดระยะเวลาในการรับชมเนื้อหาบน YouTube โดยเริ่มจากที่เรากำหนดเวลาไว้ว่าจะใช้ YouTube ต่อวัน กี่ชั่วโมง เมื่อทำการตั้งค่าแล้ว หากเราใช้เกินเวลาไอคอนแอปฯ จะกลายเป็นสีเทา และขึ้นเตือนว่าเราใช้งานเกินเวลา

### เลือกติดตาม

หรือเป็นเพื่อนกับคนที่ส่งเนื้อหาที่ดีและมีประโยชน์ ซึ่งจะช่วยให้เราได้รับเนื้อหาที่ดีและมีประโยชน์มากขึ้น

**FOLLOW**



### หากิจกรรมอื่น ๆ ทำ

แทนการเสพติดเนื้อหา เช่น ออกกำลังกาย ทำงานอดิเรก

# การมีส่วนร่วมอย่างสร้างสรรค์ ในชุมชนดิจิทัล



เทคโนโลยีดิจิทัลทำให้เราสามารถติดต่อสื่อสาร มีปฏิสัมพันธ์ เรียนรู้ แบ่งปันข้อมูลข่าวสารกันในสังคมได้อย่างสะดวกมากยิ่งขึ้น ผ่านการมีส่วนร่วมในชุมชนดิจิทัล โดยใช้เครื่องมือและแพลตฟอร์มออนไลน์ต่าง ๆ อย่างไรก็ตาม การมีส่วนร่วมในชุมชนดิจิทัล ก็มีรูปแบบการใช้ที่ไม่สมดุล และส่งผลกระทบต่อเชิงลบเช่นเดียวกัน อาทิ

1

การใช้โซเชียลมีเดียที่มากเกินไปจนความจำเป็น ทั้งด้านเวลาหรือการเผยแพร่ข้อมูล

2

การเปิดรับหรือเผยแพร่ข้อมูลเท็จหรือบิดเบือน รวมถึงการเข้าร่วมกลุ่มปิดที่มีการตีกรอบขอบเขตความเชื่อเพียงด้านเดียว ซึ่งอาจนำไปสู่การปลุกปั่นปลุกระดม

3

การคุกคามทางออนไลน์ หรือ การถูกคุกคามทางออนไลน์ ผ่านช่องทางที่หลากหลาย

4

การเสียโอกาสทางสังคม จากการใช้งานที่ไม่เหมาะสม ซึ่งอาจขยายผลกระทบไปถึงขั้นการถูกดำเนินคดีตามกฎหมาย

หลังจากที่เราได้เข้าใจถึงเรื่องการดูแล และบริหารจัดการเพื่อสุขภาพกาย สุขภาพใจ ตลอดจนการใช้งานอุปกรณ์ดิจิทัลอย่างสมดุล และภาพรวม ขั้นตอนของการมีส่วนร่วมในชุมชนอย่างสมดุลกันแล้ว ในบทถัดไปเราจะได้ เรียนรู้ลึกยิ่งขึ้น เกี่ยวกับการใช้งานเทคโนโลยีที่ส่งผลกระทบต่อ สังคม ผ่านหัวข้อ “Civic Use of Technology” การใช้เทคโนโลยีเพื่อ สังคมและตนเอง”





ปัจจุบันการใช้งานสื่อทั้งหลาย  
 มีเทคโนโลยีมากมายให้เลือกสรร  
 ใช้ให้เหมาะสมอย่างสมดุลคุณอนันต์  
 ควรจัดสรรเพื่อส่งเสริมชีวิตดี  
 เริ่มถนอมสุขภาพการยศาศาสตร์  
 อย่าพลังพลาดเสพเนื้อหาหน้าบัดสี  
 ควรจัดกาลหน้าจอไม่รอรื  
 ร่วมกันเสริมสุขศรีสร้างชุมชน



ถ้าคุณเรียนผ่านด้านนี้  
 คุณจะมีส่วนช่วย  
 ทำให้โลกออนไลน์ดียิ่งขึ้น  
 และไม่เสี่ยงทำผิดกฎหมาย  
 ที่มีโทษสูง ทั้งจำและปรับ

\*การโพสต์ต่อบุคคลอื่น ปรจงานแบบระบุชื่อ-นามสกุล ลงรูป โดยมี  
 ลักษณะเป็นการเผยแพร่ข้อความอันเป็นการหมิ่นประมาทออกไปยัง  
 สาธารณชน เป็นความผิดอาญา ฐานหมิ่นประมาทผู้อื่นด้วยการโฆษณา  
 ตามประมวลกฎหมายอาญามาตรา 326 และมาตรา 328 โทษจำคุก  
 ไม่เกิน 2 ปี และปรับไม่เกิน 2 แสนบาท

## 2.2

# CIVIC USE OF TECHNOLOGY

## วัตถุประสงค์

1. ผู้เรียนสามารถเข้าใจถึงการใช้เทคโนโลยีในการตอบโต้ แสดงความคิดเห็น มีปฏิสัมพันธ์ ติดตาม และเสพติดเนื้อหาดิจิทัลที่มีผลกระทบต่อสุขภาพจิตของตนเองและผู้อื่นได้
2. ผู้เรียนสามารถตระหนักถึงผลที่เกิดจากการมีปฏิสัมพันธ์ โดยใช้เทคโนโลยีในโลกดิจิทัลที่อาจผลมิต่ออารมณ์ ความรู้สึก และความต้องการของตนเองและผู้อื่น
3. ผู้เรียนสามารถ อธิบายผลของการเอาใจเขามาใส่ใจเราทางดิจิทัล (DIGITAL EMPATHY) ได้
4. ผู้เรียนสามารถเข้าใจถึงการสร้างค่านิยมเชิงบวกต่อชุมชนและสังคมผ่านเทคโนโลยีที่เหมาะสมได้
5. ผู้เรียนสามารถเข้าใจถึงการนำเทคโนโลยีมาใช้เพื่อพัฒนาและยกระดับคุณภาพชีวิตได้
6. ผู้เรียนสามารถเลือกใช่วิธีการค้นหาข้อมูล รวบรวม และจัดการข้อมูลที่ต้องการจากสื่อดิจิทัล

# การใช้เทคโนโลยีในโลกดิจิทัล เพื่อสังคม และตนเอง

เทคโนโลยีช่วยให้เราติดต่อสื่อสาร และมีปฏิสัมพันธ์กับผู้คนหรือสังคมได้มากขึ้น โดยมีหลากหลายรูปแบบการใช้เทคโนโลยี ซึ่งสามารถแบ่งออกเป็น

## 1 การตอบโต้

เป็นรูปแบบพื้นฐานที่สุดในการใช้เทคโนโลยีเพื่อโต้ตอบกับผู้อื่น สามารถทำได้หลายช่องทาง เช่น อีเมล แชต โดยการตอบโต้ควรมีความสุภาพ เหมาะกับกาลเทศะ 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 การเสพติด

รูปแบบการใช้เทคโนโลยีที่ส่งผลกระทบต่อชีวิตประจำวัน เช่น การใช้เวลาอยู่กับหน้าจอมากเกินไป ขาดการติดต่อกับผู้อื่น การเสพติดเทคโนโลยี เป็นปัญหาที่ควรได้รับการแก้ไข โดยควรจำกัดเวลาในการใช้เทคโนโลยี ภารกิจอื่น ๆ ทดแทน และปรึกษาผู้เชี่ยวชาญหากจำเป็น



# การจัดการผลกระทบ



## จากการใช้งานเทคโนโลยีดิจิทัล

### ผลกระทบ ทางบวก

การตอบโต้ แสดงความคิดเห็น มีปฏิสัมพันธ์ การติดตาม และเสพติด เนื้อหาดิจิทัล มีผลกระทบอย่างมีนัยสำคัญต่อทั้งบุคคลและสังคมที่เราอยู่ในปัจจุบัน ดังนั้น จึงจำเป็นต้องเข้าใจผลกระทบด้านบวกและด้านลบที่อาจเกิดขึ้น ดังนี้

01



ทำให้เราได้รับข้อมูลข่าวสาร และประสบการณ์ใหม่ จากผู้อื่น ซึ่งอาจเป็นประโยชน์ต่อการเรียนรู้ และการพัฒนาตนเอง

02



ไกลแค่ไหนก็เหมือนใกล้กัน เมื่อเทคโนโลยีทำให้การเชื่อมต่อกับผู้คน และสร้างปฏิสัมพันธ์ที่ดีได้ง่ายขึ้น สามารถพูดคุย สื่อสาร ทำกิจกรรมร่วมกันกับเพื่อน หรือสมาชิกในกลุ่มบนโลกดิจิทัลได้ แม้ว่าจะอยู่กันคนละจังหวัด หรือคนละประเทศก็ตาม

03



เทคโนโลยีช่วยให้เราแสดงความรัก ความยินดี ความห่วงใยได้ตลอดเวลา ผ่านทางรูปภาพ ข้อความ เสียง หรือคลิปวิดีโอ และยังช่วยให้สามารถเข้าไปสอบถาม เสนอทางออกในปัญหาของคนที่ต้องการ ได้ง่ายตายมากขึ้นด้วย



## ผลกระทบ ทางลบ



01



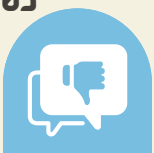
ปัญหาสุขภาพกายและสุขภาพจิต อาจเกิดขึ้นได้จากการอยู่กับหน้าจอนานเกินไป

02



ปัญหาจากสื่อที่ส่งไปไม่ครบมิติ ตัวหนังสือไม่มีเสียง ตัวอักษรไม่สามารถสื่อถึงน้ำเสียงของเราได้ หากไม่ระวังก็อาจทำให้เกิดความเข้าใจผิดหรือรู้สึกไม่ดีได้

03



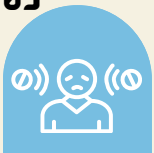
การตีความของแต่ละบุคคลต่างกัน ความขัดแย้งอาจเกิดขึ้นได้เพียงแค่อดโลกในเรื่องราวน่าเศร้า เพราะการเข้าใจผิดจากการตีความด้านลบ เมื่อเกิดความไม่พอใจก็อาจนำไปสู่อคติ และปัญหาการกลั่นแกล้งทางออนไลน์ได้

04



บนโลกออนไลน์ แทบทุกเรื่องเป็นเรื่องสาธารณะ หากเราไม่ได้ตั้งค่าจำกัดความเป็นส่วนตัว ก็เหมือนเรายืนตะโกนคุยกันอยู่ที่ริมถนน ไม่ว่าจะดีหรือร้าย คนที่อยู่รอบ ๆ ก็จะรับรู้ไปด้วย ถึงแม้เขาจะทำได้ไม่สนใจ แต่บางเรื่องก็ทำให้ตัวเรานั้นเกิดความอับอาย จนกลายเป็นตัวเร่งความขัดแย้งให้เกิดไว้มากขึ้น เรียกว่า "หน้าต่างมีหู ประตूमืดตา" ของแท้

05



ไม่กล้าบอกออกไป เมื่อเราเห็นคนส่วนมากพูด หรือคอมเมนต์ไปในทางเดียวกัน แต่เรามีความเห็นที่ตรงกันข้าม ก็อาจทำให้เราตัดสินใจเก็บความเห็น หรือปัญหาเหล่านั้น เอาไว้คนเดียว เพราะคิดว่าคงไม่มีใครเห็นด้วยกับเรา

06



ได้รับข้อมูลข่าวสารที่ผิด อาจส่งผลเสียต่อการตัดสินใจ หรือการดำเนินชีวิต

## แนวทางการใช้เทคโนโลยีอย่างเหมาะสม

เพื่อหลีกเลี่ยงผลกระทบด้านลบ สิ่งสำคัญคือต้องรู้จักใช้เทคโนโลยี อย่างเหมาะสม ดังนี้

### 1) สุขภาพและมีมารยาทไว้ก่อน

การตอบโต้ หรือแสดงความคิดเห็นบนโลกดิจิทัล ควรหลีกเลี่ยงการใช้ถ้อยคำที่รุนแรง ไม่สุภาพ และล้ำเส้นความเป็นส่วนตัว

### 2) ตระหนักว่าโลกดิจิทัลกว้างใหญ่ไร้ขีดจำกัด

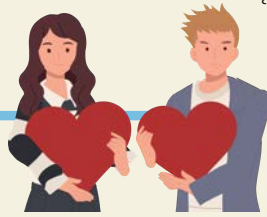
ผู้คนที่เข้ามาอ่าน มาแสดงความคิดเห็นนั้นมีความหลากหลาย ทั้งระดับความรู้ ทักษะคิด และความเชื่อ ย่อมมีคนเห็นต่าง และเกิดความขัดแย้งได้ อย่าเพิ่งด่วนดีใจหรือเศร้าใจมากจนเกินความจริง

### 3) อย่าให้ความคิดเห็นของเราตัดสินคนอื่น

ข้อความของเราอาจทำให้ผู้อื่นได้รับความเสียหายได้ ในบางครั้งความรู้หรือแนวคิดที่เราเชื่อมั่น อาจจะทำให้คนอื่นรู้สึกอึดอัด ไปจนถึงรู้สึกไม่ดีกับเราก็ได้

## เข้าอกเข้าใจกัน ผ่าน Digital Empathy

แม้การสื่อสารบนโลกดิจิทัล ยากที่จะถ่ายทอดและรับรู้อารมณ์ความรู้สึกระหว่างกัน แต่ไม่ได้แปลว่ามันไม่มีอยู่ และในทางตรงกันข้าม มันอาจถูกขยายทวีคูณความรู้สึกได้ด้วยเช่นกัน ความดีใจถูกขยาย ความเจ็บปวดใจก็ถูกขยาย จึงเป็นเหตุให้เราต้องใส่ใจกับอีกเครื่องมือที่สำคัญในโลกดิจิทัล สิ่งนั้นเรียกว่า **Digital Empathy**



## Digital Empathy

### หรือ การเอาใจเขามาใส่ใจเราทางดิจิทัล

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

1

เข้าใจผลกระทบของการแสดงออกผ่านโลกออนไลน์ที่มีต่อผู้อื่น

โดยเฉพาะในด้านความรู้สึก และการส่งอิทธิพลต่อความคิดหรือพฤติกรรม



2

เคารพมุมมอง และอารมณ์ที่หลากหลายเมื่อเข้าสู่การปฏิสัมพันธ์บนโลกออนไลน์



3

แสดงออกซึ่งความเห็นอกเห็นใจผู้อื่นบนโลกออนไลน์

ทั้งด้านอารมณ์ ความจำเป็น ความต้องการ ความกังวลใจ และความใส่ใจ



## แนวทางการพัฒนาทักษะ Digital Empathy

### 1. เป็นนักฟังอย่างตั้งใจ

มองให้ลึกกว่าแค่ตัวอักษร อีโมจิ หรือสติ๊กเกอร์ ที่ไม่สามารถเล่าเรื่องและบริบทได้ทั้งหมด แต่ให้นึกถึงสิ่งที่อยู่เบื้องหลังการสื่อสารเหล่านั้น

### 2. เป็นนักมองต่างมุม

ฝึกให้เชี่ยวชาญการมองจากมุมมองของผู้อื่น โดยเฉพาะในโลกออนไลน์ที่กำแพงทางภูมิศาสตร์พังทลายลง

### 3. เป็นนักสื่อสารที่รอบคอบ

สารบนออนไลน์ ง่ายจะถูกตีความผิด ดังนั้น ฟังลึกถึงการเสียดสีใช้อีโมจิอย่างระวัง และอ่านทวนซ้ำก่อนกด "ส่ง"

### 4. เป็นนักเชื่อในส่วนดี

เมื่อรู้สึกเป็นฝ่ายถูกกระทำ หรือเห็นอะไรที่ดูโง่โงวมอง ให้คิดไว้ก่อนว่าอีกฝ่ายนั้นมีเจตนาที่ดี รวมไปถึงชนวนเหตุของการทะเลาะ เช่น การไม่กดอ่าน อ่านไม่ตอบ ตอบช้าไม่ทันใจนั้น คุณไม่มีทางรู้ว่าสถานการณ์ "โลกจริง" ในขณะนั้นของอีกฝ่ายเป็นอย่างไร เพียงแค่เฝ้าดูจากจอที่มองเห็นแค่โลกออนไลน์

## 5. เป็นนักเคารพความเห็นต่าง

แม้จะไม่เห็นด้วยกับเขา จงแสดงออกถึงท่าทีแห่งความรู้โดยเคารพ และให้เกียรติในสิทธิการแสดงความคิดเห็น รวมทั้ง การรู้จักและเข้าใจ อารมณ์ของตัวเองในทุกขณะ

## 6. ระวังตลกร้าย มุกไม่ขำ

“คุณฮา แต่คนอื่นไม่จำเป็นต้องฮา” โดยเฉพาะถ้ามุกนั้น ไม่ใช่แค่แป๊ก แต่ยังสามารถทำร้ายจิตใจหรือสร้างความแตกแยกได้

## 7. ระวังอุบัติเหตุทางดิจิทัล

"แมวมิมพ์" "แบตหมด" "เน็ตหลุด" "ลืมตั้งเตือน" "ใส่ผิดวัน" ฯลฯ ล้วนมีโอกาสเกิดขึ้นได้เสมอ ในยุคที่มนุษย์ต้องพึ่งพา "อุปกรณ์" ในการสื่อสาร ระวังการแสดงออกหรือสร้างความรู้สึกดตันจากเฉพาะ มุมมองของตนเอง ไม่เพียงทำร้ายจิตใจ แต่ยังอาจทำลายความสัมพันธ์อัน มีค่า

## 8. สะสมคลังคำสะท้อนอารมณ์

ยิ่งเราสื่อสารกับคนหลากหลาย เรา ยิ่งต้องใส่ใจที่จะเข้าใจและไวต่อ คำสื่อความรู้สึกทั้งหลายเพื่อเราจะหยิบใช้ได้เหมาะสมทั้งในบทบาท ของผู้ฟังและผู้พูดไม่ต่างกับการเรียนรู้ภาษาใหม่ เหมือนคนที่เข้าใจทั้ง ภาษากลาง และภาษาถิ่น ก็จะมีทักษะในการเข้าอกเข้าใจคนจำนวนมากขึ้น

## เจออย่างนี้...รับมืออย่างไร ?

เราลองมาดูกันดีกว่าว่า ถ้าเราต้องเจอกับสถานการณ์ที่กระทบต่อความรู้สึก และความต้องการจากเนื้อหาที่มีคนสื่อสาร หรือปฏิสัมพันธ์บนโลกดิจิทัล จะจัดการอย่างไร เพื่อให้ผู้รับสบายใจ และผู้ให้รู้สึกดีกัน

กรณีที่ 01

คนใกล้ชิด หรือสนิทสนม ที่เคยหยอกล้อกัน โพสต์ข้อความ หรือภาพที่สื่อถึงความสิ้นหวัง หมดกำลังใจ

ไม่ควรทำ



โพสต์ หรือแสดงความคิดเห็นหยอกล้อให้รู้สึกสนุกสนาน เนื่องจากตัวหนังสือไม่มีน้ำเสียงและสื่อความรู้สึกได้ลำบาก อาจจะตีความหมายที่จะสื่อสารผิดได้ อีกทั้งการตอบโต้ของเรานอกจากจะปรากฏแก่เพื่อนเจ้าของโพสต์แล้ว เพื่อนของเพื่อนที่ติดตามก็เห็นด้วย แม้ว่าเพื่อนเราจะเข้าใจ แต่คนอื่นอาจไม่เข้าใจ และอาจมีการตอบโต้กันไปมา

ควรทำ



โพสต์ หรือแสดงความคิดเห็นอย่างจริงจัง และตรงไปตรงมา หากรู้สึกเป็นห่วง ให้บอกความรู้สึกไปตรง ๆ ตระหนักอยู่เสมอว่า เราไม่เพียงแค่อสื่อสารกับคน ๆ นั้นเท่านั้น แต่ยังมีอีกหลายคนซึ่งเป็นเพื่อนของเขา หรืออาจจะเป็นใครก็ได้เห็นข้อความของเรา และตีความหมายไปต่าง ๆ นานา ตามประสบการณ์ของเขาเอง ระวังไว้ก่อนที่จะแสดงความคิดเห็นอะไรไป เพราะจากห่วงใยอาจกลายเป็นดราม่าได้

## กรณีที่ 02

น้องชายที่เรามองว่า ไม่ค่อยตั้งใจเรียน โพสต์ข้อความว่า  
ตกงาน ไม่มีงานทำ และกำลังหางานในภาวะเศรษฐกิจตกต่ำ

## ไม่ควรทำ



โพสต์ หรือคอมเมนต์สั่งสอน หลายครั้งเมื่อเห็นภาพหรือข้อความลูกหลาน  
ที่ไม่ได้ตั้งใจ อาจจะแสดงอารมณ์โกรธ หงุดหงิด ฉุนเฉียว หรืออยากสั่ง  
สอน แล้วโต้ตอบด้วยข้อความหรือสื่อที่ไม่เหมาะสม ในเชิงลดทอนกำลังใจ  
หรือซ้ำเติม แต่ไม่ได้ประสงค์ร้าย และทำด้วยความเป็นห่วงด้วยซ้ำ แต่เราก็  
เคยทำอะไรผิดพลาดหรือไม่ใช่คนสมบูรณ์แบบกันทั้งนั้น

## ควรทำ



โพสต์ หรือคอมเมนต์ให้กำลังใจและพร้อมสนับสนุน หรือให้คำแนะนำใน  
ช่องทางส่วนตัว





# การใช้เทคโนโลยีอย่างเหมาะสม เพื่อสร้างค่านิยมเชิงบวกต่อชุมชน และพัฒนาคุณภาพชีวิต



## ค่านิยมเชิงบวกในการใช้เทคโนโลยีให้เหมาะสม

### 1) ความรับผิดชอบ

รับผิดชอบต่อการกระทำของตน ตระหนักถึงผลกระทบต่อผู้อื่น และสังคม

### 2) ความเคารพ

เคารพความแตกต่าง และวัฒนธรรมของผู้อื่น ไม่ใช้เทคโนโลยี เพื่อละเมิดหรือกลั่นแกล้งผู้อื่น

### 3) ความสามัคคี

ใช้เทคโนโลยีเพื่อเชื่อมโยงเข้าหากัน สร้างสัมพันธ์อันดี ช่วยเหลือเกื้อกูลกัน

เพื่อให้ค่านิยมเชิงบวกต่อชุมชน และสังคมมีความยั่งยืน จึงควรปฏิบัติตาม

## แนวทางการใช้เทคโนโลยีให้เหมาะสมด้วยตัวเอง

### 1) ตระหนักถึงผลกระทบของการกระทำของตนเอง

ควรคิดถึงผลจากการกระทำของตนเอง ก่อนที่จะโพสต์ข้อความ หรือแชร์ข้อมูลใด ๆ บนโลกออนไลน์

### 2) ให้ความเคารพผู้อื่น

ไม่ใช่คำพูดหรือการกระทำที่เป็นการเหยียดหยามหรือล่วงละเมิดผู้อื่น

### 3) ใช้เทคโนโลยีอย่างสร้างสรรค์

ใช้เพื่อสร้างสรรค์สิ่งใหม่ ๆ เป็นประโยชน์ต่อชุมชนและสังคม

### 4) มีส่วนร่วมในกิจกรรมเพื่อสังคม

สร้างความสัมพันธ์ที่ดีและช่วยเหลือซึ่งกันและกัน เช่น การบริจาคเงินหรือสิ่งของ การให้ความช่วยเหลือผู้ประสบภัย หรือการสนับสนุนโครงการเพื่อสังคม

## ตัวอย่างการใช้เทคโนโลยีที่เหมาะสม เพื่อส่งเสริมค่านิยมเชิงบวกต่อชุมชนและสังคม

#### 1) ใช้เทคโนโลยีเพื่อการศึกษา

เรียนรู้สิ่งใหม่ ๆ พัฒนาความรู้ความสามารถของตนเอง และแบ่งปันความรู้กับผู้อื่นได้

#### 2) ใช้เทคโนโลยีเพื่อช่วยให้ทำงาน

อย่างมีประสิทธิภาพมากขึ้น และสามารถทำงานร่วมกับผู้อื่นจากทั่วโลกได้

#### 3) ใช้เทคโนโลยีเพื่อการทำงานอาสา

สามารถใช้เทคโนโลยีเพื่อช่วยเหลือผู้อื่น แก้ปัญหาในชุมชน และสร้างสังคมที่ดีขึ้น

# ผลกระทบที่เกิดขึ้นจาก การใช้เทคโนโลยีที่ไม่เหมาะสม

เราต้องระมัดระวังผลกระทบที่เกิดขึ้นจากการใช้เทคโนโลยีที่ไม่เหมาะสม ซึ่งสามารถแบ่งออกได้เป็น 3 ประเภทหลัก ๆ ดังนี้

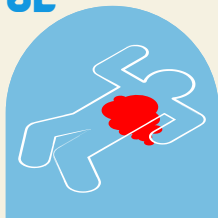
01



## ผลกระทบต่อตัวผู้ใช้ ได้แก่

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

02



## ผลกระทบต่อผู้อื่น ได้แก่

- ปัญหาอาชญากรรม เช่น การหลอกลวง การโจรกรรม ข้อมูล การเผยแพร่ข้อมูลเท็จ
- ปัญหาสังคม การแพร่กระจายเนื้อหาที่ไม่เหมาะสม เช่น สื่อลามกอนาจาร ความรุนแรง เหยียดเชื้อชาติ เป็นต้น

03



## ผลกระทบต่อสังคม ได้แก่

- ปัญหาสิ่งแวดล้อม เช่น การใช้พลังงานไฟฟ้ามากเกินไป ปัญหาขยะอิเล็กทรอนิกส์
- ปัญหาเศรษฐกิจ เช่น การสูญเสียงาน ปัญหาความเหลื่อมล้ำทางสังคม เป็นต้น

## แนวทางในการสร้างความตระหนักถึงผลกระทบ



### ที่เกิดขึ้นจากการใช้เทคโนโลยีที่ไม่เหมาะสม

ขอแนะนำแนวทางในการสร้างความตระหนัก ถึงผลกระทบที่เกิดขึ้นจากการใช้เทคโนโลยีที่ไม่เหมาะสม ได้แก่

#### 1) การให้ความรู้และความเข้าใจ

เกี่ยวกับผลกระทบของการใช้เทคโนโลยีที่ไม่เหมาะสม

#### 2) การปลูกฝังค่านิยมและจริยธรรม

ในการใช้เทคโนโลยี และหลีกเลี่ยงการใช้เทคโนโลยีในทางที่ก่อให้เกิดโทษ

#### 3) การพัฒนากฎหมายและกฎระเบียบที่เกี่ยวข้อง

เพื่อคุ้มครองผู้ใช้เทคโนโลยีและสังคมจากผลกระทบที่อาจเกิดขึ้น

อีกอย่างที่สำคัญคือต้องรู้จักเลือกรับเนื้อหาที่เหมาะสม เพื่อให้ได้รับข้อมูล ที่ถูกต้อง และจะได้ไม่เผยแพร่ข้อมูลที่อาจก่อให้เกิดผลเสียสู่สังคม



## ประโยชน์การใช้เทคโนโลยี เพื่อยกระดับคุณภาพชีวิต

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 หรือคอมพิวเตอร์ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ก็สามารถเริ่มต้นขายสินค้าได้ทันที เช่น การให้บริการขนส่ง ผู้คนสามารถให้บริการขนส่งสินค้าหรือผู้โดยสารได้ โดยใช้รถยนต์หรือรถจักรยานยนต์ของตนเอง

การรับจ้างทำงานผ่านแพลตฟอร์มต่าง ๆ ปัจจุบันมีแพลตฟอร์มมากมาย ที่ให้บริการรับจ้างทำงาน ผู้คนสามารถสมัครใช้บริการเหล่านี้เพื่อหางานทำ เช่น งานเขียนบทความ งานออกแบบ งานแปล งานกราฟิก เป็นต้น

### 3) การยกระดับคุณภาพชีวิต



- **การเข้าถึงบริการสาธารณสุขได้สะดวกและรวดเร็วขึ้น** การนัดหมายแพทย์ออนไลน์ ช่วยให้ผู้คนสามารถนัดหมายแพทย์ได้โดยไม่ต้องเดินทางไปโรงพยาบาล ประหยัดเวลาในการรอคอย และช่วยให้วางแผนในการเดินทางได้ง่ายขึ้น
- **การตรวจสุขภาพทางไกล** ปัจจุบันผู้คนสามารถปรึกษาแพทย์และรับการรักษาได้จากที่บ้าน โดยไม่ต้องเดินทางไปโรงพยาบาล

นอกจากนี้ เทคโนโลยียังช่วยให้ผู้คนสามารถดูแลสุขภาพตนเองได้มากขึ้น เช่น ดูปลิปสออนอกกำลังกาย หรือใช้แอปพลิเคชันติดตามสุขภาพที่จะคอยติดตามสุขภาพของเรา เช่น อัตราการเต้นของหัวใจ ระดับน้ำตาลในเลือด ปริมาณแคลอรีที่บริโภค หรืออุปกรณ์ติดตามการออกกำลังกายที่ช่วยนับจำนวนก้าวที่เดิน ระยะทางที่วิ่ง หรือระยะเวลาที่ออกกำลังกาย เป็นต้น

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 ความถูกต้องของข้อมูล และแหล่งอ้างอิง การสืบค้นข้อมูลจากสื่อดิจิทัล เป็นทักษะที่จำเป็นสำหรับทุกคน อย่างไรก็ตาม เราควรใช้ทักษะนี้อย่างชาญฉลาด ตรวจสอบความถูกต้องของข้อมูลและแหล่งที่มาของข้อมูลอย่างรอบคอบ เพื่อไม่ให้ถูกหลอกลวงหรือตกเป็นเหยื่อของข้อมูลเท็จ



## เครื่องมือในการค้นหาข้อมูลจากสื่อดิจิทัล

### เครื่องมือที่ใช้ในการค้นหาข้อมูลทั่วไป

- **Google Search (Google):**

เป็นเครื่องมือค้นหาที่แพร่หลายที่สุด มีความสามารถในการค้นหาโดยใช้ อัลกอริทึมที่ทันสมัย

- **Microsoft Bing :**

เป็นเครื่องมือค้นหาอีกตัวที่มีความสามารถในการค้นหาข้อมูลทั่วไป และรูปภาพ

- **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

สำหรับการค้นหาข้อมูลในหนังสือและสื่อพิมพ์ 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 ให้กระชับ 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.dsd.go.th**

### ค้นโดยให้มีคำค้นทุกคำในแหล่งเดียว

ให้ใส่คำค้นทุกคำที่ต้องการโดยเว้นวรรคระหว่างคำค้น ตัวอย่าง สมัครงาน กราฟิก ชื่องานตรี

### ค้นโดยใช้คำช่วย OR

กรณีอยากให้ได้ข้อมูลเพิ่มมากขึ้นเกี่ยวกับคำค้นหลัก ตัวอย่าง สมัครงาน กราฟิก OR 2D animator

### ใส่เครื่องหมายคำพูด

กรณีต้องการให้มีทั้งประโยคในแหล่งข้อมูล ตัวอย่าง "Work from Home"

### ใส่เครื่องหมายลบ

เพื่อกรองคำที่ไม่ต้องการออก โดยใส่ คำค้น - คำที่ต้องการกรองออก ตัวอย่าง กราฟิก - ตัดต่อ

### แปลงหน่วยต่าง ๆ

โดยพิมพ์ ตัวเลข หน่วยก่อนแปลง เท่ากับ หน่วยหลังแปลง อย่างเช่น แปลงค่าเงิน ตัวอย่าง คำค้น 100 บาท เท่ากับ ดอลลาร์

### แสดงเวลาเปรียบเทียบ

เวลา ประเทศที่ 1 ประเทศที่ 2 ตัวอย่าง เวลา ไทย อเมริกา

เพียงเท่านี้เราก็จะสามารถสืบค้นข้อมูลได้อย่างตรงใจมากขึ้น !



## TIP

# เคล็ดลับการค้นหาข้อมูลออนไลน์ คุณเคยลองแล้วหรือยัง?

(เรียบเรียงจากข้อมูลคำแนะนำของ Google Gemini)



## เทคนิคขั้นพื้นฐาน

### 1. ใช้คำค้นหาที่เฉพาะเจาะจง

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

### 2. ใช้เครื่องหมายคำพูด ("")

เช่น "คำว่ารักไม่เคยแพ้อะไร" เพื่อค้นหาเฉพาะวลีนั้น

### 3. ใช้เครื่องหมายลบ (-)

เช่น "รถยนต์ - มือสอง" เพื่อไม่ให้แสดงผลที่เกี่ยวข้องกับรถยนต์มือสอง

### 4. ใช้เครื่องหมายบวก (+)

เช่น "ข่าว + ดิจิทัลไอดี" เพื่อบังคับให้มีคำว่า "ดิจิทัลไอดี" 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  
ไม่หลงเชื่อในครั้งแรกที่เห็น

**9. ใช้คำพ้องความหมาย**

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

**10. ใช้เครื่องหมายดอกจัน (\*)**

เช่น "วิธีทำ\*ผัดไทย" เพื่อค้นหาสูตรอาหารผัดไทยทุกประเภท



## เทคนิคขั้นสูง



### 1. ใช้ประโยชน์จากฟังก์ชัน autocomplete

พิมพ์แค่คำหรืออักษรต้น แล้วลองไล่ดูคำที่เครื่องมือค้นหาแนะนำให้มา

### 2. เรียนรู้คีย์ลัด

เช่น Ctrl+F เพื่อค้นหาคำในหน้าเว็บ หรือ Ctrl+T เพื่อเปิดแท็บใหม่

### 3. ใช้เครื่องมือบุ๊กมาร์ก

เก็บเว็บไซต์ที่เป็นประโยชน์ไว้ดูภายหลัง

### 4. อัปเดตความรู้การค้นหายู่เสมอ

ติดตามข่าวสารและเทคนิคใหม่ ๆ รวมทั้งการใช้ AI ในการสืบค้นเรียบเรียงข้อมูล

### 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**

ไม่จำกัดอยู่แค่เว็บไซต์ ลองค้นหาในหนังสือ วารสาร หรือฐานข้อมูลอื่น ๆ

**10. ค้นหาด้วยเสียง**

ใช้การค้นหาด้วยเสียงเมื่อสะดวก

**11. ใช้การค้นหาด้วยรูปภาพ**

อัปโหลดรูปภาพเพื่อค้นหาข้อมูลที่เกี่ยวข้อง

**12. ใช้เครื่องมือค้นหาสำหรับการช้อปปิ้ง**

เช่น Google Shopping เพื่อเปรียบเทียบราคาสินค้า

**13. ใช้เครื่องมือค้นหาสำหรับการท่องเที่ยว**

เช่น Kayak หรือ Skyscanner เพื่อค้นหาตั๋วเครื่องบินและโรงแรม

**14. ใช้เครื่องมือค้นหาสำหรับการเรียน**

เช่น Google Scholar หรือ JSTOR สำหรับบทความวิชาการ

**15. ใช้เครื่องมือค้นหาสำหรับการหางาน**

เช่น LinkedIn หรือ Indeed

**16. ใช้เครื่องมือค้นหาสำหรับการเรียนภาษา**

เช่น Duolingo หรือ Memrise

**17. ใช้เครื่องมือค้นหาสำหรับการค้นหาสูตรอาหาร**

เช่น Yummly หรือ Allrecipes



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  
 สร้างสรรค์ก่อแหล่งสื่อสารโยงสังคม  
 ทั้งตอบโต้ติดตามความนิยม  
 ร่ายคารมความเห็นคอมเมนต์กัน  
 สิ่งสำคัญสร้างไมตรีไร้ปัญหา  
 ใช้ภาษาด้วยเข้าใจกันและกัน  
 ค่านิยมสามัคคีผูกสัมพันธ์  
 ร่วมแบ่งปันสืบค้นข้อเท็จจริง

# 2.1 Balanced Use of Technology

พฤติกรรม  
การใช้เทคโนโลยี  
ของคนไทย

ส่งผลดีต่อคนไทย  
ในหลายด้าน

การจัดการ  
การใช้เทคโนโลยี

การมีส่วนร่วม  
อย่างสร้างสรรค์  
ในชุมชนดิจิทัล

รูปแบบการใช้ที่ไม่สมดุล

การใช้โซเชียลมีเดีย  
ที่มากเกินไปจนกลายเป็น

การเปิดรับหรือเผยแพร่  
ข้อมูลเท็จหรือบิดเบือน

การคุกคามทางออนไลน์

การเสียโอกาสทางสังคม

การดูแลสุขภาพ  
บนโลกดิจิทัล  
(Digital Health)

สุขภาพกาย

- ดวงตา
- หู
- ร่างกาย
- การนอนหลับ
- สุขภาพโดยรวม

สุขภาพจิต

- จัดการอารมณ์  
และความรู้สึก
- ใส่ใจความสัมพันธ์  
ที่มีคุณค่า
- รู้ทันพฤติกรรม  
การใช้เทคโนโลยี

แนวทางป้องกันสุขภาพจิต

การเหนื่อยล้าจากการใช้งานดิจิทัล

การบริหารจัดการ  
เวลาบนโลกดิจิทัล

การใช้เวลาหน้าจอดิจิทัล

ต้นเหตุแห่งอาการเสพติดหน้าจอ

ผลกระทบจากการเสพติดหน้าจอ

ผลกระทบ  
ต่อร่างกาย

ผลกระทบ  
ต่อการดำเนินชีวิต

เครื่องมือที่ช่วยจัดสรรเวลา  
การใช้เทคโนโลยีดิจิทัล

การเสพติดเนื้อหา  
ส่งผลเสียต่อสุขภาพจิต

ด้านอารมณ์

ด้านความสัมพันธ์

ด้านพฤติกรรม

ลักษณะเนื้อหาที่ควรพิจารณา  
เพื่อป้องกันการเสพติดเนื้อหา  
ที่ไม่เหมาะสม

การจัดการ  
และตั้งค่าการเข้าถึงเนื้อหา

# 2.2

## Civic Use of Technology

**การใช้เทคโนโลยีในโลกดิจิทัล เพื่อสังคม และตนเอง**

**การสืบค้นข้อมูลจากสื่อดิจิทัล**

**การใช้เทคโนโลยีอย่างเหมาะสม**

รูปแบบการใช้เทคโนโลยี

การจัดการผลกระทบจากการใช้งานเทคโนโลยีดิจิทัล

- ผลกระทบทางบวก
- ผลกระทบทางลบ

แนวทางการใช้เทคโนโลยีอย่างเหมาะสม

การเอาใจเขามาใส่ใจเราทางดิจิทัล

แนวทางการพัฒนาทักษะ Digital Empathy

การรับมือกับสถานการณ์ที่กระทบต่อความรู้สึก

- ไม่ควรทำ
- ควรทำ

ค่านิยมเชิงบวกในการใช้เทคโนโลยีให้เหมาะสม

แนวทางการใช้เทคโนโลยีให้เหมาะสมด้วยตัวเอง

ตัวอย่างการใช้เทคโนโลยีที่เหมาะสม

ผลกระทบที่เกิดขึ้นจากการใช้เทคโนโลยีที่ไม่เหมาะสม

แนวทางในการสร้างความตระหนักถึงผลกระทบ

ประโยชน์การใช้เทคโนโลยีเพื่อยกระดับคุณภาพชีวิต

การสืบค้นข้อมูลจากสื่อดิจิทัลอย่างมีประสิทธิภาพ

เครื่องมือในการค้นหาข้อมูลจากสื่อดิจิทัล

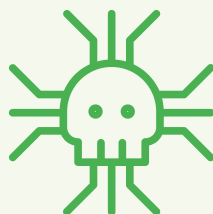
เทคนิคการค้นหาข้อมูลจากสื่อดิจิทัลอย่างไรให้ตรงใจ

เคล็ดลับการค้นหาข้อมูลออนไลน์

- เทคนิคขั้นพื้นฐาน
- เทคนิคขั้นสูง



03



## การจัดการความปลอดภัย ในโลกดิจิทัล

— Digital Security —



# แนะนำสำหรับผู้สอน

## • วัตถุประสงค์

ผู้เรียนมีความรู้เกี่ยวกับ ความเสี่ยง การป้องกัน หรือการจัดการ ภัยคุกคามทางไซเบอร์ได้

## • ขอบเขตของเนื้อหาตอนนี้

### 3.1 Behavioral Cyber-Risk Management

- ความปลอดภัยเริ่มที่การปกป้อง “ส่วนบุคคล” วันที่สอน  
/.../...
- การล่วงละเมิดทางไซเบอร์ (Cyber Abuse) วันที่สอน  
/.../...
- ภัยคุกคามทางไซเบอร์ (Cyber Threat) วันที่สอน  
/.../...
- ออนไลน์อย่างไรให้ปลอดภัย ? วันที่สอน  
/.../...

## • ขอบเขตของเนื้อหาตอนนี้

### 3.2 Organizational Cyber-Risk Management

- First Jobber ควรรู้ไว้! วันที่สอน  
/.../...
- ความเสี่ยงจากการใช้เทคโนโลยีในองค์กร วันที่สอน  
/.../...
- แนวปฏิบัติเพื่อร่วมกันป้องกันภัยไซเบอร์ระดับองค์กร วันที่สอน  
/.../...
- กฎหมายที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ในประเทศไทย  
วันที่สอน  
/.../...

เวลาในการเรียน



# รู้ศัพท์ ไม่ลับสน



1



## SOCIAL ENGINEERING

หรือ วิศวกรรมสังคม

คือ เป็นศิลปะการหลอกลวงผู้คน เพื่อผลประโยชน์ตามที่แฮกเกอร์ต้องการ โดยใช้วิธีการทางจิตวิทยาในการหลอกล่อ

2



## TECHNICAL ATTACKS

คือ ภัยคุกคามจากผู้มีความรู้ด้านระบบคอมพิวเตอร์เครือข่าย และข้อมูลทางอิเล็กทรอนิกส์

3



## RANSOMWARE

คือ ภัยคุกคามทางไซเบอร์ที่ทำการเข้ารหัสหรือล็อกไฟล์ ไม่ว่าจะป็นไฟล์เอกสาร รูปภาพ วิดีโอ โดยผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลย หากไฟล์เหล่านั้นถูกเข้ารหัส และเพื่อกู้ข้อมูลคืน ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏ

4



## SYNTHETIC CONTENT

หรือ ข้อมูลสังเคราะห์

คือข้อมูลที่ไม่ได้สร้างขึ้นโดยมนุษย์ ซึ่งเลียนแบบข้อมูลในโลกแห่งความเป็นจริง ข้อมูลประเภทนี้จะสร้างขึ้นจากอัลกอริทึม การประมวลผล และการจำลองโดยใช้เทคโนโลยีปัญญาประดิษฐ์ ช่วยสร้าง

# รู้ศัพท์

# ไม่ลับสน



5



## SCAMS

คือ ลักษณะการหลอกลวงในรูปแบบต่างๆ ผ่านระบบอินเทอร์เน็ต

6



## WATERMARK

หรือลายน้ำ

คือ การแสดงความเป็นเจ้าของรูปภาพหรือเอกสารนั้น ๆ โดยลายน้ำจะมีลักษณะที่เป็นรูปภาพจางๆ ที่สามารถไปวางบนส่วนใดของรูปภาพหรือข้อความก็ได้

7



## PASSKEY

คือ เป็นวิธีลงชื่อเข้าบัญชีผู้ใช้ในเว็บไซต์หรือในแอปพลิเคชันโดยพิสูจน์ตัวผู้ใช้ (AUTHENTICATION) โดยไม่ต้องมีรหัสผ่าน



ถ้าคุณเรียนผ่านด้านนี้  
คุณจะรู้จัก  
เข้าใจและป้องกันตนเอง  
จากภัยคุกคามทางไซเบอร์ ได้

## 3.1

# BEHAVIORAL CYBER-RISK MANAGEMENT

## วัตถุประสงค์

1. ผู้เรียนสามารถตระหนักถึงความเสี่ยงหรือความไม่ปลอดภัยที่อาจเกิดขึ้นบนโลกดิจิทัล
2. ผู้เรียนรู้วิธีการออนไลน์ให้ปลอดภัยและตั้งรหัสผ่านอย่างไรให้ปลอดภัย
3. ผู้เรียนสามารถเข้าใจถึงการป้องกันหรือการจัดการภัยคุกคามทางไซเบอร์ได้

## ได้อย่างไร ? เราจึงจะปลอดภัยในโลกดิจิทัล

ไม่มีสิ่งใดสิ่งเดียวจะเป็นคำตอบได้ เหมือนกับการขับขี้นานพาหนะบนท้องถนน ที่ความปลอดภัยไม่ได้ถูกกำหนดโดยฝ่ายใดฝ่ายเดียว

ดังนั้น การรับประกันความปลอดภัยในโลกดิจิทัลจึงเป็นความร่วมมือกันของแต่ละบุคคล ตลอดจนองค์กร และระบบในภาพรวม

ในหลักสูตร EDC Plus ด้านที่ 3 นี้ เราจะร่วมกันมองไปที่ 2 ส่วนสำคัญอันเป็นรากฐานของการสร้างความปลอดภัยในโลกดิจิทัลให้เกิดขึ้นทั้งต่อตนเอง และสังคม

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

ถัดจากนั้น เราจะขยายวงสู่การป้องกันตนให้พ้นจากการถูกโจมตีทางไซเบอร์ ในฐานะที่เราแต่ละคน ล้วนอยู่ในบทบาทปกป้ององค์กร พร้อมเทคนิคความปลอดภัยออนไลน์ง่าย 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 ตลอดจนเชื่อมโยงสู่ผลลัพธ์ทางร่างกายและชีวิตทรัพย์สิน

ข่าวร้ายคือ หากเราไม่ตระหนัก บางครั้งเราอาจกลายเป็นผู้ล่วงละเมิดผู้อื่นโดยไม่ตั้งใจ

### การคุกคามทางไซเบอร์

เป็นการกระทำที่ก่อความเสียหายต่อทรัพย์สิน ระบบ อุปกรณ์ ซึ่งอาจเรียกได้ว่าเป็นการโจมตี

ที่น่าเสียดายคือ หลายครั้งความเสียหายเกิดขึ้น เพราะช่องโหว่ที่เราเปิดไว้เอง เหมือนกับรถยนต์ที่เปิดประตูค้างไว้แถมยังเสียบกุญแจเอาไว้ให้ด้วย

# การล่วงละเมิดทางไซเบอร์ (Cyber Abuse)



## การล่วงละเมิดทางไซเบอร์ (Cyber Abuse)

คือ การใช้เทคโนโลยีดิจิทัลเพื่อคุกคาม ช่มชู้ หรือก่อกวนผู้อื่นในทางที่เป็นอันตราย หรือไม่เหมาะสม

## รูปแบบการล่วงละเมิดทางไซเบอร์

สามารถเกิดขึ้นในหลายรูปแบบ เช่น

### 1. การคุกคามทางอิเล็กทรอนิกส์ (Cyberstalking)



การติดตามหรือก่อกวนผู้อื่นอย่างต่อเนื่องผ่านช่องทางออนไลน์ จนทำให้ผู้ถูกติดตาม หรือถูกก่อกวน รู้สึกถูกคุกคามหรือไม่ปลอดภัย เช่น

#### EXAMPLE

ไอดอลสาวเจอแฟนคลับชายคนเดิมทุกที่ที่ไป เขาติดตามข้อมูลสถานที่เกี่ยวกับไอดอลโพสต์แล้วติดตามไปทุกที่ แกรมยังทำเหมือนบังเอิญเจอ ทำให้ไอดอลสาวรู้สึกไม่ปลอดภัยจนต้องแจ้งความ

## 2. การเปิดเผยข้อมูลส่วนตัว (Doxxing)



การเปิดเผยหรือแพร่กระจายข้อมูลส่วนตัว รูปภาพ คลิปวิดีโอ หรือข้อมูลที่ละเอียดอ่อนของบุคคลอื่น โดยไม่ได้รับอนุญาต เช่น

### EXAMPLE

**การล่าแม่มดหรือคนที่ไม่ชอบบนโลกออนไลน์ โดยทำการขุดรูปเก่า ๆ ข้อมูลที่อยู่ ที่ทำงาน บุคคลรอบตัวออกมาเปิดเผย**

## 3. การกลั่นแกล้งทางไซเบอร์ (Cyberbullying)



การใช้แพลตฟอร์มออนไลน์เพื่อข่มขู่ ล้อเลียน หรือทำร้ายผู้อื่น ทั้งในด้านจิตใจและอารมณ์

## 4. การใช้คำพูดเกลียดชัง (Hate Speech)



คือการเผยแพร่หรือแสดงความคิดเห็นที่มีเนื้อหาเกลียดชัง ล่วงละเมิด หรือเลือกปฏิบัติต่อบุคคล ซึ่งไม่ได้จำกัดแค่คำพูด แต่รวมไปถึงสื่อทุกชนิด และไม่ได้จำกัดเพียงแค่การใช้ถ้อยคำหยาบคาย ด่าทอ ถูกเหยียดหยาม เท่านั้น แต่รวมถึงความตั้งใจทำให้ผู้อื่นเข้าใจผิด โน้มน้าวชักจูงให้เกลียดชังเป้าหมาย ตลอดจนการลดทอนศักดิ์ศรีและคุณค่าความเป็นมนุษย์

## สาเหตุของการล่วงละเมิดทางไซเบอร์

มีหลายปัจจัยที่ซับซ้อน และเกี่ยวข้งกัน ดังนี้

### 1. ความไม่ระบุดัตตน :

อินเทอร์เน็ตและโซเชียลมีเดียมักให้ความไม่ระบุดัตตนแก่ผู้ใช้ ซึ่งอาจทำให้บางคนรู้สึกว่ พวกเขาสามารถทำการล่วงละเมิดคนอื่นได้ โดยไม่ต้องรับผิดชอบต่อการกระทำของตนเอง

### 2. ขาดการควบคุม :

บางครั้งแพลตฟอร์มออนไลน์ อาจขาดกลไกการควบคุมที่เหมาะสม เพื่อป้องกันการล่วงละเมิดทางไซเบอร์

### 3. ขาดความเข้าใจและการศึกษา :

ผู้ใช้บางคนอาจไม่เข้าใจถึงผลกระทบ หรือความรุนแรงของการกระทำของตนต่อผู้อื่น หรือไม่รู้จักวิธีการใช้เทคโนโลยีอย่างมีความรับผิดชอบ

### 4. ความแตกต่างทางสังคมและวัฒนธรรม :

ความขัดแย้งหรือความไม่เข้าใจระหว่างกลุ่มคน หรือวัฒนธรรมต่าง ๆ

### 5. รู้สึกไม่พึงพอใจหรือถูกทอดทิ้ง :

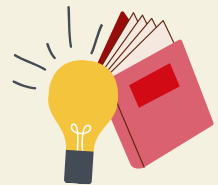


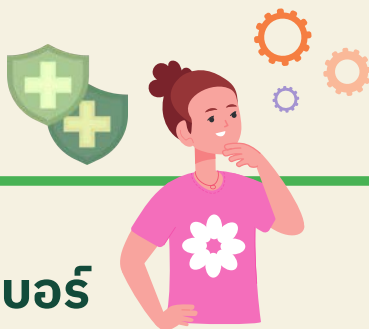
คนที่มีความรู้สึกไม่พึงพอใจหรือถูกทอดทิ้ง อาจใช้การละเมิดทางไซเบอร์ เป็นวิธีแสดงความไม่พอใจ หรือแสวงหาความสนใจ

### 6. ความหวาดกลัวและความไม่แน่นอน :



ในสถานการณ์ที่มีความหวาดกลัว เช่น ระหว่างวิกฤตหรือการเปลี่ยนแปลงทางสังคม บางคนอาจหันไปใช้การล่วงละเมิดทางไซเบอร์ เพื่อแสดงออก หรือเพื่อจัดการกับความรู้สึกของตน





## รับมือการคุกคามทางไซเบอร์

แม้ปัจจัยจะหลากหลายจนดูเหมือนเป็นเรื่องยากที่จะจัดการ แต่สำหรับใครที่ได้เรียนรู้ผ่านมาถึงจุดนี้ คงมีแนวทางสร้างเกราะป้องกันสำหรับตนเองไว้บ้างแล้ว

ทั้งด้วยการตระหนักว่า มีโอกาสที่เราอาจจะพบเจอการล่วงละเมิด หากมีใครพยายามเริ่มต้นการล่วงละเมิด เราควรรู้ทันและหลีกเลี่ยง

ขณะเดียวกัน ควรตั้งค่าความเป็นส่วนตัวบนอุปกรณ์ที่ใช้ให้อยู่ในระดับที่เราต้องการ และระมัดระวังการเปิดช่อง เผยแพร่ หรือแชร์ข้อมูลส่วนตัว ซึ่งอาจจะกลายเป็นเชื้อไฟตั้งต้นให้กับคนก่อการล่วงละเมิด



### WARNING

หากเราไม่ระวัง เราอาจกลายเป็นผู้ที่ล่วงละเมิดผู้อื่นได้โดยไม่รู้ตัว วิธีพื้นฐานที่จะป้องกันไม่ให้หลงพลาดพลั้ง เราควรหมั่นก่อร่างสร้าง “ความเข้าอกเข้าใจในโลกดิจิทัล” หรือ Digital Empathy ไว้ให้มันคง [โดยสามารถติดตามเรื่องนี้ได้ในด้านที่ 2.2 เข้าอกเข้าใจกันผ่าน Digital Empathy]

# ภัยคุกคามทางไซเบอร์ (Cyber Threat)



ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง การกระทำใด ๆ ที่มีความตั้งใจที่จะทำลาย บุกกรุก หรือทำให้ระบบคอมพิวเตอร์ ข้อมูลดิจิทัล หรือเครือข่ายการสื่อสารต่าง ๆ ได้รับความเสียหาย ซึ่งอาจมาจากบุคคล กลุ่ม หรือแม้กระทั่งประเทศที่มีเจตนาทำร้าย

## รูปแบบภัยคุกคามทางไซเบอร์ ในระดับส่วนตัว

แบ่งได้เป็น 2 กลุ่ม คือ กลุ่มที่ใช้ กลยุทธ์ “วิศวกรรมทางสังคม” หรือ **Social Engineering** หรือเรียกง่าย ๆ ว่า “ล่อ-ลวง-หลอก” กับอีกกลุ่มหนึ่งใช้ **วิธีทางเทคนิค** หรือบางกรณีก็เป็นการใช้ทั้งสองวิธีร่วมกัน เช่น “หลอกให้เชื่อ เพื่อให้เหยื่อติดตั้งแอป”

สำหรับรูปแบบภัยคุกคามทางไซเบอร์ ในระดับส่วนตัว มีเทคนิคน่าสนใจที่ควรรู้ทัน อาทิ

## กลยุทธ์ทางวิศวกรรมสังคม (Social Engineering)

- ลวงให้กรอกข้อมูล (Phishing Scams)

การส่งอีเมล หรือสร้างเว็บไซต์ปลอมแปลงเลียนแบบของค์กรที่น่าเชื่อถือ เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลส่วนตัว เช่น หลอกให้กรอกรหัสผ่าน เลขบัตรเครดิต



- หลอกให้ดีใจ (Lottery or Prize Scam)

หลอกให้เหยื่อเชื่อว่า ชนะรางวัล แต่สุดท้ายต้องจ่ายเงิน โหลดแอปฯ หรือมอบข้อมูลส่วนบุคคล

- หลอกให้รัก (Romance Scam)

หลอกให้รัก แล้วออกอุบายเพื่อให้เหยื่อหลงเชื่อโอนเงินให้



- หลอกให้ลงทุน (Investment Scam)

หลอกให้ลงทุน โดยกล่าวอ้างอย่างน่าเชื่อว่าจะได้รับผลตอบแทนสูง

### • สวมรอยหลอก (Pretexting)

การสร้างสถานการณ์ปลอมขึ้นมา เพื่อให้เหยื่อไว้ใจ และยอมเปิดเผยข้อมูลส่วนตัว เช่น ปลอมเป็นฝ่ายเทคนิคการสนับสนุน ปลอมเป็นเจ้าของหน้าที่ตำรวจ



### • วางเหยื่อล่อ (Baiting)

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



### • ชูกรรโชก (Scareware)

การสร้างความเร่งด่วน ปลอมแปลงสถานการณ์ให้เหยื่อรู้สึกกลัว เช่น แจ้งเตือนว่าบัญชีของคุณถูกบุกรุก ข้อมูลของคุณรั่วไหล เพื่อกดดันให้เหยื่อตัดสินใจผิดพลาด เช่น คลิกลิงก์ที่ไม่ปลอดภัยหรือดาวน์โหลดโปรแกรมรักษาความปลอดภัยปลอม



### • Mining Social Media

การเรียนรู้และเก็บรวบรวมข้อมูลจากกิจกรรมบนโลกออนไลน์ของเหยื่อ เพื่อนำมาสร้างชุดข้อมูลสำหรับใช้ทำให้เหยื่อหลงเชื่อได้ง่ายขึ้น

## กลยุทธ์การโจมตีทางเทคนิค(Technical Attacks)

- มัลแวร์ (Malware)

สร้างแอปหรือซอฟต์แวร์ที่ไม่พึงประสงค์สามารถติดตั้งบนอุปกรณ์โดยไม่รู้ตัว ทำหน้าที่ขโมยข้อมูล ทำลายอุปกรณ์ หรือควบคุมอุปกรณ์ของเราได้



- การโจมตีแบบ Watering Hole

ฝังมัลแวร์ในเว็บไซต์ที่กลุ่มเป้าหมายมักเข้าใช้งานบ่อย ๆ เพื่อให้อุปกรณ์ของเหยื่อติดตั้งมัลแวร์ทันทีที่เข้าใช้งาน

- การโจมตีแบบ Zero-Day

การใช้ช่องโหว่ของซอฟต์แวร์โจมตี ก่อนที่จะมีแก้ไขช่องโหว่ การโจมตีลักษณะนี้ป้องกันได้ยาก



## สาเหตุของภัยคุกคามทางไซเบอร์

เกิดจากหลายสาเหตุที่ซับซ้อนและเชื่อมโยงกัน ปัจจัยต่าง ๆ เหล่านี้ ส่งผลให้เกิดความเสี่ยงและช่องโหว่ ที่ผู้โจมตีสามารถใช้ประโยชน์ เพื่อทำการโจมตีทางไซเบอร์ได้ ต่อไปนี้คือบางสาเหตุหลักของภัยคุกคามทางไซเบอร์

### 1. อินเทอร์เน็ตสามารถซ่อนตัวตนได้

โดยการทำโปรไฟล์ปลอมขึ้นมา ทำให้บางคนรู้สึกว่าจะสามารถกระทำการไม่เหมาะสม โดยไม่ต้องเผชิญกับผลที่ตามมาได้



### 2. หลายการโจมตีทางไซเบอร์มีจุดประสงค์เพื่อการฉ้อโกงทางการเงิน

เช่น การเรียกค่าไถ่ผ่าน Ransomware

### 3. องค์กรบางแห่งอาจใช้การโจมตีทางไซเบอร์เพื่อขโมยความลับทางการค้า

หรือข้อมูลที่เป็นประโยชน์ทางการแข่งขัน



### 4. บางประเทศอาจใช้การโจมตีทางไซเบอร์เพื่อแทรกแซงการเมือง

โดยขโมยข้อมูลของหน่วยงานสำคัญ ที่ส่งผลกระทบต่อระดับประเทศ

5. ซอฟต์แวร์และฮาร์ดแวร์ที่มีช่องโหว่  
ทำให้ผู้โจมตีสามารถเจาะระบบได้



6. ผู้ใช้หลายคนอาจไม่มีความรู้  
เกี่ยวกับความปลอดภัยไซเบอร์  
ทำให้พวกเขาตกเป็นเป้าหมายที่  
ง่ายต่อการโจมตี

7. การเติบโตอย่างรวดเร็ว  
ของเทคโนโลยีทำให้เกิดช่องโหว่ใหม่ ๆ  
ที่ผู้โจมตีสามารถใช้ประโยชน์ได้



**EXAMPLE**

## สายชอปต้องระวัง ! ตัวอย่างภัยออนไลน์ ที่มาพร้อมกับ ONLINE SHOPPING

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

## EXAMPLE

- มัลแวร์และไวรัส : การคลิกลิงก์หรือดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่ปลอดภัย อาจนำไปสู่การติดตั้งมัลแวร์บนอุปกรณ์
- เว็บไซต์บางแห่งอาจเก็บข้อมูลส่วนบุคคลมากกว่าที่จำเป็น ซึ่งอาจนำไปสู่ความเสี่ยงหากข้อมูลนั้นถูกขโมย

ทุกวันนี้การซื้อของออนไลน์ แทบจะกลายเป็นส่วนหนึ่งในชีวิตประจำวันของเราไปแล้ว แต่ก็ต้องให้ระวังภัยร้ายที่อาจซ่อนอยู่ในรูปแบบของการขายสินค้าเหล่านี้ด้วย ก่อนการสั่งซื้อของออนไลน์ทุกครั้ง ต้องพิจารณาความน่าเชื่อถือของร้าน เพื่อป้องกันการถูกฟิชซิง ที่หลอกให้เรากรอกข้อมูลส่วนตัวหรือข้อมูลบัตรเครดิตลงไป และถ้าหากรู้สึกว่าร้านให้กรอกข้อมูลเกินความจำเป็น ให้หยุดการกรอกข้อมูลทั้งหมดทันที ไม่เช่นนั้น อาจจะถูกดูดเงินได้

หรือบางครั้งอาจได้ของไม่ตรงปก ผิดสี ผิดขนาด ไม่เป็นอย่างที่คิดไว้ จะเคลมหรือร้องเรียนก็ไม่สามารถติดต่อร้านได้

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

## แหล่งข้อมูลเพื่อติดตามสถานการณ์

### ภัยคุกคามไซเบอร์

ในประเทศไทย มีหลายหน่วยงานที่ให้ข้อมูลและอัปเดตเกี่ยวกับสถานการณ์ภัยคุกคามทางไซเบอร์ ซึ่งรวมถึงการแจ้งเตือน การวิเคราะห์ และคำแนะนำเกี่ยวกับวิธีป้องกันแหล่งข้อมูลเหล่านี้ เป็นทรัพยากรที่ดีสำหรับองค์กรและบุคคลในภาคธุรกิจ รวมไปถึงประชาชนทั่วไปที่ต้องการรักษาความปลอดภัยในโลกไซเบอร์ เช่น

#### • ไทยเซิร์ต (THAICERT)

หน่วยงานรับผิดชอบ ด้านการตอบสนองเหตุการณ์คอมพิวเตอร์ฉุกเฉินของประเทศไทย ให้ข้อมูลและการแจ้งเตือน เกี่ยวกับภัยคุกคามทางไซเบอร์ รวมถึง มีบทความและคำแนะนำเกี่ยวกับการป้องกัน

#### • สำนักงานคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

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

หน่วยงานที่รับผิดชอบในการกำหนดนโยบายและแผนงานเพื่อเสริมสร้างความมั่นคงไซเบอร์ของประเทศ รวมทั้ง การติดตาม ประเมินภัยคุกคาม และตอบสนองเพื่อรับมือกับภัยคุกคามทางไซเบอร์

- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

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

มีบทบาทในการกำกับดูแลธุรกิจบริการดิจิทัล ควบคู่ไปกับการส่งเสริมและพัฒนาการทำธุรกรรมอิเล็กทรอนิกส์ในประเทศไทย อย่างมั่นคงปลอดภัย

- กองบัญชาการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี

(บช.สอท.) หรือเป็นที่รู้จักในชื่อ "กองบัญชาการตำรวจไซเบอร์"

เป็นหน่วยงานหลักในการสืบสวนสอบสวนคดีอาชญากรรมทางเทคโนโลยี ที่มีผลกระทบต่อประชาชน

- เว็บไซต์และบล็อกด้านความปลอดภัยไซเบอร์

มีเว็บไซต์และบล็อกหลายแห่ง ที่ให้ข้อมูลอัปเดตเกี่ยวกับภัยคุกคามทางไซเบอร์และการป้องกัน ซึ่งเป็นทรัพยากรที่ดีสำหรับผู้ที่สนใจเรื่องความปลอดภัยไซเบอร์

การติดตามแหล่งข้อมูลเหล่านี้ช่วยให้ผู้คนและองค์กรต่าง ๆ สามารถอัปเดตตัวเองกับข้อมูลล่าสุดเกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการป้องกัน ช่วยให้สามารถรักษาความปลอดภัยของข้อมูลและระบบของตนได้

# ออนไลน์อย่างไร



## ให้ปลอดภัย ?



**TIP**

การใช้อินเทอร์เน็ต และแพลตฟอร์มออนไลน์อย่างปลอดภัย เป็นสิ่งสำคัญในยุคดิจิทัล เพื่อป้องกันตัวเองจากภัยคุกคามทางไซเบอร์ และรักษาความเป็นส่วนตัว โดยมีคำแนะนำพื้นฐาน เกี่ยวกับวิธีการใช้อินเทอร์เน็ตอย่างปลอดภัย ดังนี้

**1**

สร้างรหัสผ่านที่ยากต่อการทาย



โดยควรตั้ง Password ให้ปลอดภัย ด้วยคอนเซ็ปต์ “ไม่ซ้ำ ไม่ง่าย ไม่บอก”

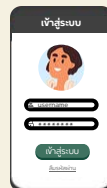
- 1) รหัสผ่านควรมีความยาวอย่างน้อย 8 ตัวอักษร
- 2) ใช้ตัวอักษรพิมพ์ใหญ่ ตัวอักษรพิมพ์เล็ก ตัวเลข และสัญลักษณ์พิเศษ ผสมกัน
- 3) อย่าใช้ข้อมูลส่วนบุคคล เช่น วันเกิด ชื่อสัตว์เลี้ยง หรือนามสกุล
- 4) ไม่ใช่คำที่มีในพจนานุกรม
- 5) อย่าใช้รหัสผ่านเดียวกันกับหลายบัญชี
- 6) ใช้โปรแกรมจัดการรหัสผ่านที่ซับซ้อนเพื่อสร้างและเก็บรหัสผ่าน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



2

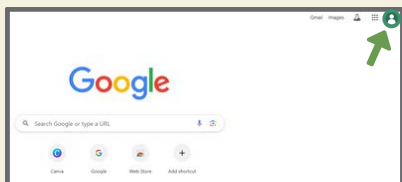
ใช้การตรวจสอบสิทธิ์ 2 ขั้นตอน

(Two-Factor Authentication: 2FA)



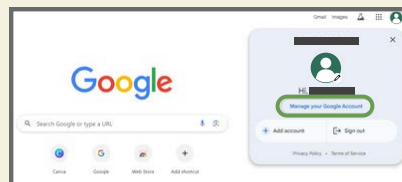
ขั้นตอนที่ 1

กดที่ภาพโปรไฟล์มุมบนขวา

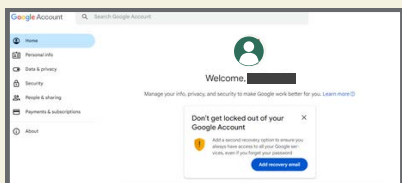


ขั้นตอนที่ 2

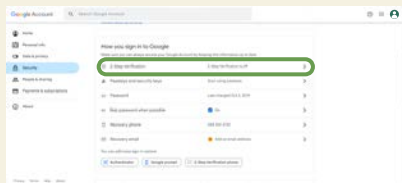
กด จัดการบัญชี Google



ขั้นตอนที่ 3

เลือกตัวเลือก ความปลอดภัย  
จากเมนูด้านซ้าย

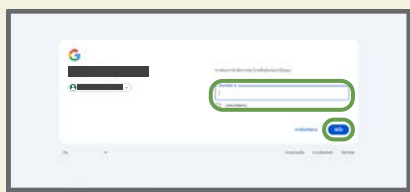
ขั้นตอนที่ 4

เลือก การยืนยันตัวตน  
แบบสองขั้นตอน



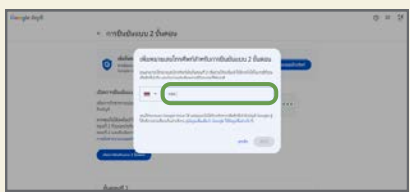
### ขั้นตอนที่ 5

กด เริ่มต้นใช้งาน และใส่รหัสผ่านบัญชี จากนั้นกด ถัดไป



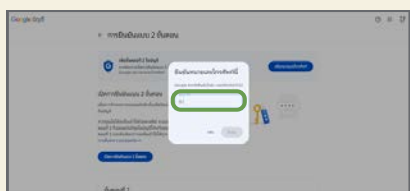
### ขั้นตอนที่ 6

กรอก เบอร์โทรศัพท์ เพื่อยืนยันตัวตน



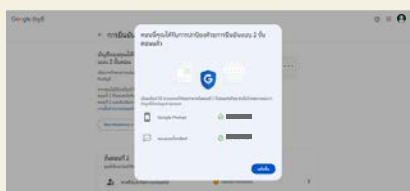
### ขั้นตอนที่ 7

ใส่รหัสที่ส่งเข้ามาจากเบอร์มือถือ



### ขั้นตอนที่ 8

กด เปิด เพื่อทำการเปิดการยืนยันตัวตน 2 ขั้นตอน





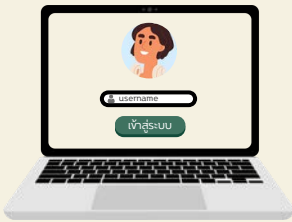
ในปัจจุบันมีการพัฒนามาตรฐานใหม่ขึ้นมาทดแทนการยืนยันตัวตนด้วยรหัสผ่าน (Password) สิ่งนั้นเรียกว่า **Paskey**

## Paskey

เป็นระบบการยืนยันตัวตนโดยไม่ใช้รหัสผ่าน แต่ใช้ระบบหลังบ้านของผู้ให้บริการในการดำเนินการตามขั้นตอนทางเทคนิค ก่อนจะให้ผู้ใช้ยืนยันตัวตนด้วยการชีวมิติ เช่น การสแกนนิ้ว หรือสแกนใบหน้า บนอุปกรณ์ส่วนตัวของผู้ใช้

### EXAMPLE

#### ตัวอย่างเช่น



1

เมื่อเราต้องการจะเข้าสู่เว็บไซต์ที่เคยเป็นสมาชิก ระบบ Paskey ของเว็บไซต์นั้น จะสอบถาม ชื่อผู้ใช้งานที่คุ้นเคย



2

แต่เมื่อเข้าสู่ขั้นตอนถัดไป เว็บไซต์จะแสดงรหัส QR Code ให้ผู้ใช้สแกนด้วยโทรศัพท์มือถือที่ลงทะเบียนไว้

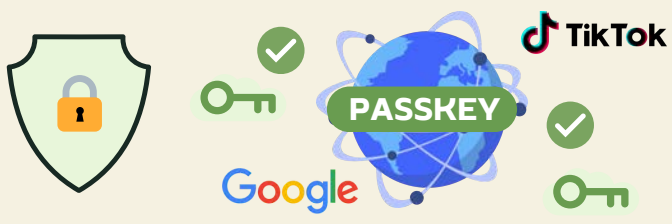
EXAMPLE



3

อาจจะใช้การสแกนนิ้วหรือสแกนหน้าได้ทันที

- ระบบการยืนยันตัวตนด้วย Passkey นี้ จะปลอดภัยกว่าระบบอื่น ๆ เช่น ไม่ต้องก๊อปปี้รหัสผ่านหายแล้วโดนสวมรอยหรือโดนคนร้ายหลอกให้ส่งเลข OTP รวมทั้ง ผู้ให้บริการก็ไม่ต้องกังวลว่า ข้อมูลรหัสผ่านจะรั่วหรือถูกเจาะอีกด้วย
- ขณะนี้เริ่มมีบริษัทระดับโลกหลายแห่งเปิดให้เลือกใช้ Passkey ในการยืนยันตัวตนแล้ว หากเป็นไปได้ แนะนำให้เรียนรู้ และลองตั้งค่าการใช้งาน เพื่อความปลอดภัยที่เข้มแข็งขึ้น





TIP

3

ระมัดระวังการคลิกลิงก์ สแกน หรือ ดาวนโหลดไฟล์ อย่าไวใจแหล่งที่ไม่น่าเชื่อถือ



เพราะลิงก์หรือการสแกน เป็นจุดเริ่มต้นสำคัญ ที่คนร้ายมักจะใช้เพื่อพาเราเข้าไปติดกับดัก ซึ่งกับดักอาจจะมาในรูปแบบเว็บไซต์ปลอม หรือ แอปพลิเคชันปลอม อย่างไรก็ตาม ถ้าพึงการคลิกลิงก์หรือสแกนเพียงอย่างเดียว ไม่ได้ทำให้โดนมิจฉาชีพดูดเงินทันที แต่การเข้าไปกรอกข้อมูลส่วนตัว หรือกดดาวนโหลดแอปพลิเคชันนอกสโตร์ ที่ไม่ผ่านการรับรองต่างหาก ที่ทำให้มิจฉาชีพได้ข้อมูลไปใช้ในการดูดเงินหรือใช้มือถือเราเองในการโอนเงินหรือข้อมูลไปให้ที่ที่เขาต้องการ

4

หมั่นอัปเดตซอฟต์แวร์ และระบบปฏิบัติการอยู่เสมอ



เพื่อป้องกันจากช่องโหว่ที่อาจถูกโจมตี

5

ระมัดระวังในการใช้ Wi-Fi สาธารณะ

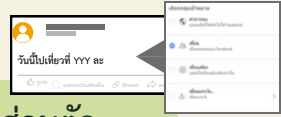


หลีกเลี่ยงการทำธุรกรรมทางการเงิน หรือการเข้าถึงข้อมูลสำคัญเมื่อใช้ Wi-Fi สาธารณะ บางกรณีอาจพิจารณาใช้ VPN (Virtual Private Network) เพื่อเพิ่มความปลอดภัย



6

## ตรวจสอบและปรับการตั้งค่าความเป็นส่วนตัว



บนโซเชียลมีเดีย แอปฯ และบริการออนไลน์อื่น ๆ เพื่อควบคุมข้อมูลที่แชร์

7

## ระมัดระวังการแชร์ข้อมูลส่วนบุคคล



เช่น ที่อยู่บ้าน วันเกิด หรือหมายเลขประจำตัวประชาชนในอินเทอร์เน็ต

8

## สำรองข้อมูลอยู่เสมอ



ในอุปกรณ์ที่ไม่ได้เชื่อมต่อกับเครื่องคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ

9

## หมั่นอัปเดตสถานการณ์



เพื่อสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ล่าสุดและวิธีการป้องกัน



หากถามถึงความเสี่ยงโลกไซเบอร์  
 อาจเจาะเจอเริ่มจากภัยส่วนตัว  
 มาหลากหลายรูปแบบพาตีนกลัว  
 หมายมองมั่วลวงละเมิดแก๊งก่อวณ  
 ทั้งยังมีภัยคุกคามล่อลวงหลอก  
 กลิ้งกลับกลอกด้วยเทคนิคเป็นขบวน  
 ไม่ประมาทตั้งรหัสให้ครบถ้วน  
 กันป่วนปวนใช้สองชั้นพาสคีย์ป้องกันเอย



ถ้าคุณเรียนผ่านด้านนี้  
คุณจะเป็นส่วนหนึ่ง  
ที่ช่วยให้องค์กรไม่ตกอยู่ใน  
ความเสี่ยงจากการโจมตี  
ทางไซเบอร์ ได้

## 3.2

# ORGANIZATIONAL CYBER-RISK MANAGEMENT

## วัตถุประสงค์

1. ผู้เรียนสามารถเข้าใจถึงการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น และความตระหนักในภัยคุกคามได้
2. ผู้เรียนสามารถเข้าใจถึงการป้องกันหรือการจัดการภัยคุกคามทางไซเบอร์ได้

# First Jobber

## ควรรู้ไว้!



ถ้าคุณเป็นคนที่กำลังจะก้าวเข้าสู่การทำงานอย่างเต็มตัว คุณควรรู้ไว้ว่า การบริหารความเสี่ยงมีความสำคัญอย่างยิ่งต่อความสำเร็จและความยั่งยืนขององค์กร ซึ่งเราควรรู้ไว้ก่อนจะสมัครงานบริษัทนั้น เพื่อให้เราเข้าใจพื้นฐานของแนวความคิดในการจัดการความเสี่ยงขององค์กร





WARNING

# ความเสี่ยงจากการใช้เทคโนโลยีในองค์กร



ความเสี่ยงในระดับองค์กรถือเป็นสิ่งที่จะต้องมีการจัดการอย่างรอบคอบ โดยความเสี่ยงหลัก ๆ จากการใช้เทคโนโลยีในองค์กร มีดังนี้

1

ความเสี่ยงด้านความปลอดภัยจากการโจมตีทางไซเบอร์



สามารถทำให้องค์กรสูญเสียข้อมูลสำคัญ การเข้าถึงระบบถูกขัดขวาง หรือเกิดความเสียหายต่อระบบ IT ได้

2

การรั่วไหล หรือการสูญหายของข้อมูลลับ และข้อมูลส่วนบุคคล



สามารถนำไปสู่ความเสียหายทางกฎหมาย ความสูญเสียทางการเงิน และความเสียหายต่อชื่อเสียงได้

3

การขาดความมั่นคงและความพร้อมในการใช้งานของระบบ IT



สามารถนำไปสู่การหยุดชะงักของการดำเนินงาน ความล่าช้า และความเสียหายต่อการดำเนินงานขององค์กร



## WARNING

4

ความเสี่ยงจากการไม่ปฏิบัติตามกฎหมายและข้อกำหนด



เช่น กฎหมาย PDPA สามารถนำไปสู่ความรับผิดทางกฎหมาย และทำให้ชื่อเสียงเสียหายได้

5

ความเสี่ยงจากการใช้งานเทคโนโลยีส่วนบุคคลในการทำงาน (Bring Your Own Device)



การใช้อุปกรณ์ส่วนบุคคล สำหรับการทำงาน สามารถเพิ่มความเสี่ยงจากการรั่วไหลของข้อมูล และการโจมตีทางไซเบอร์

6

การขาดการฝึกอบรมและความตระหนักรู้ของพนักงาน



หากพนักงานขาดการฝึกอบรมเกี่ยวกับความปลอดภัยไซเบอร์ อาจทำให้เกิดความเสี่ยงจากการคลิกลิงก์ที่เป็นอันตราย หรือการเปิดเผยข้อมูลโดยไม่ระมัดระวัง

7

ความเสี่ยงจากการพึ่งพาผู้ให้บริการภายนอก



เช่น การพึ่งพาซอฟต์แวร์ บริการคลาวด์ หรือผู้ให้บริการ IT ภายนอก อาจเพิ่มความเสี่ยง หากไม่มีการจัดการ และการตรวจสอบที่เหมาะสม

## EXAMPLE

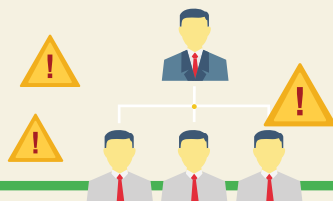
## WORLD ECONOMIC FORUM (WEF)

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 กลายเป็นตัวเร่งให้ข้อมูลสังเคราะห์หรือข้อมูลเทียม จากเทคโนโลยี AI หรือ Synthetic Content กระจายไปได้อย่างรวดเร็ว สามารถเข้าแทรกแซงทำลายระบบเศรษฐกิจ ทำให้สังคมเกิดความแตกแยก เกิดความไม่ไว้วางใจในแหล่งข้อมูล ทั้งจากสื่อและภาครัฐ เหล่าโซเชียลมีเดียแพลตฟอร์มต่าง ๆ จะพบกับความยากลำบากในการนำเสนอข้อมูลที่น่าเชื่อถือ

นอกจากนี้ ยังมีภัยที่จะเกิดจากเทคโนโลยี AI ที่จะกลายเป็นปัจจัยเสี่ยงติด TOP 10 ในอีก 10 ปีข้างหน้าด้วยเช่นกัน



## รูปแบบความเสียหายไซเบอร์ต่อองค์กร

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

**การโจมตีต่อองค์กร** ผู้โจมตีมีเป้าหมายสำคัญ เช่น

**เงินและทรัพย์สิน หรือสิ่งที่เปลี่ยนเป็นเงินได้**

เป็นหนึ่งในสาเหตุหลักของการโจมตีทั้งปวง

**ข้อมูล**

อาจเพื่อโจรกรรมข้อมูลเพื่อนำไปขายต่อ หรือด้วยวัตถุประสงค์อื่น ๆ เช่น ฐานข้อมูลผู้ใช้ ไฟล์เนื้อหาที่เป็นความลับ

**ทำลายชื่อเสียง**

อาจเป็นการโจมตี เพื่อให้องค์กรเป้าหมายเสียชื่อเสียง

**อุดมการณ์**

หลายครั้งผู้โจมตีอ้างเหตุผลอุดมการณ์ อย่างไรก็ตาม ก็มีความเป็นไปได้ว่าจะมีเรื่องอื่น ๆ เป็นสาเหตุร่วมด้วย

## กลยุทธ์ทางวิศวกรรมสังคม (Social Engineering)

### อีเมลหลอกให้กด หลอกให้กรอก (Phishing Scams)



การส่งอีเมลปลอมแปลงเลียนแบบองค์กรภายใน เพื่อหลอกให้พนักงานเปิดเผยข้อมูลสำคัญหรือสิทธิ์เข้าถึงระบบ

### สร้างเรื่องหลอกลวง (Pretexting)



การสร้างสถานการณ์ปลอมขึ้นมาเพื่อให้เข้าถึงสถานที่หรือระบบขององค์กร เช่น ปลอมตัวเป็นพนักงานส่งของหลอกลวงเจ้าหน้าที่รักษาความปลอดภัย

### ปลอมตัวเป็นคนกลาง (Man-in-the-Middle Attack)



การหลอกลวงพนักงาน ให้เปิดเผยช่องทางเข้าถึงระบบเครือข่ายขององค์กร จากนั้นคนร้ายจะสามารถดักจับข้อมูลการสื่อสารระหว่างทางแล้วปลอมตัวเป็นคนกลาง เพื่อหลอกลวงทั้งฝ่ายต้นทางและปลายทาง เช่น ปลอมเป็นคนกลางระหว่างการเจรจาซื้อขายสินค้าล็อตใหญ่ เพื่อให้ผู้ซื้อหลงโอนเงินไปที่คนร้าย 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 ที่เข้ารหัสข้อมูลของเหยื่อและเรียก ransomware เพื่อถอดรหัส สิ่งนี้สามารถส่งผลกระทบร้ายแรงต่อองค์กรเนื่องจากสามารถหยุดชะงักการดำเนินงานและก่อให้เกิดความสูญเสียทางการเงินอย่างมีนัยสำคัญ

# แนวปฏิบัติเพื่อร่วมกันป้องกัน ภัยไซเบอร์ระดับองค์กร



นอกจากการระมัดระวังการใช้เทคโนโลยีแบบส่วนตัวแล้ว พนักงานในองค์กรยังต้องเรียนรู้การใช้เทคโนโลยีในองค์กรอย่างเหมาะสม ตามนโยบายและรู้เท่าทัน โดยจัดแบ่งแนวปฏิบัติเป็น 4 กลุ่มใหญ่ ๆ ได้แก่

## 1. ตระหนักระวังภัย ((คน))

- ไม่เชื่อง่าย ไม่ตกเป็นเหยื่ออุบายลวงให้กรอก หลอกให้กดต่าง ๆ
- มีวินัยในการจัดเก็บและใช้รหัสผ่านที่แข็งแรง ใช้ระบบยืนยันตัวตนสองขั้นตอนเสมอ (หากมี)
- พิสูจน์และยืนยันตัวตนเสมอ เมื่อจำเป็นต้องมีการเปิดเผยข้อมูลสำคัญ ส่งไฟล์ หรือโอนเงิน
- ให้ความสำคัญกับการจัดการสิทธิ์การเข้าถึงไฟล์ อุปกรณ์ หรือระบบขององค์กร
- ไม่ระวังแค่ภัยบนออนไลน์ เพราะคนร้ายอาจมาในรูปแบบการบุกรุกมาเข้าถึงข้อมูลสำคัญ หรือหลอกมอບอุปกรณ์ เพื่ออาศัยเราเป็นทางผ่านในการโจมตีได้

## 2. เกาะติดนโยบาย



- รู้จัก เข้าใจ และปฏิบัติตามนโยบายด้านความปลอดภัยไซเบอร์ขององค์กร
- อัปเดต อัปสกิล ติดตามข่าวสาร และเข้าร่วมการอบรมเกี่ยวกับความปลอดภัยไซเบอร์ การใช้เทคโนโลยีอย่างรับผิดชอบ เพื่อสร้างความตระหนักรู้ และยกระดับทักษะในการป้องกันภัย
- เป็นหูเป็นตา รายงานเสมอ หากพบเหตุการณ์หรือกิจกรรมเสี่ยงภัยไซเบอร์ในองค์กร ไม่ว่าจะเป็นการส่งสัยการโจมตีจากภายนอก 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. รัศกุ่มด้านเทคนิค



- อยู่ในมาตรฐานของมาตรการรักษาความปลอดภัยไซเบอร์ขององค์กร
- เช่น ไม่แอบติดตั้งแอปฯ หรืออุปกรณ์โดยไม่ได้รับอนุญาต
- หมั่นอัปเดตซอฟต์แวร์ แอนตี้ไวรัส และระบบปฏิบัติการเป็นรุ่นใหม่
- ฝึกหัดการตั้งค่าความสามารถด้านการรักษาความปลอดภัยอยู่เสมอ
- ไม่ละเลยคำเตือนที่ปรากฏบนแอปฯ หรือระบบต่าง ๆ
- ใช้เว็บไซต์และแอปพลิเคชันให้ชำนาญ เพื่อไม่ตกเป็นเหยื่อการหลอกลวง

#### 4. พร้อมรับหากภัยมา



- คิดไว้เสมอว่า เรามีโอกาสโดนโจมตีได้ทุกเมื่อ และเตรียมแผนสำรองที่สมเหตุสมผล
- สำรองข้อมูล สำรองระบบ สำรองอุปกรณ์ เพื่อให้มีความ “ยืดหยุ่น” หรือ Resilience แม้มีการโจมตี แต่ก็ยังไม่เสียหายหนักจนต้องหยุดกิจการ
- ใช้หลัก BACK UP 3-2-1 คือ จัดเก็บข้อมูลสำคัญอย่างน้อย 3 ชุด ให้อยู่ในอย่างน้อย 2 รูปแบบสื่อ (เช่น มีทั้งคลาวด์ และในฮาร์ดดิสก์) และมีอย่างน้อย 1 ชุด จัดเก็บอยู่นอกสถานที่





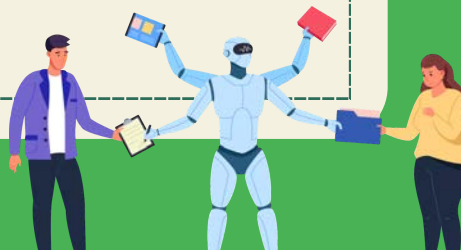
## TIP

## Update ประเด็นความปลอดภัยทางไซเบอร์ ที่ทั่วโลกให้ความสำคัญ



เทคโนโลยี AI ได้มีการพูดถึงในการประชุมหลาย ๆ เวที จากระดับนานาชาติ ซึ่งหลายประเทศต่างให้ความสำคัญ รวมถึง ประเทศไทย และเริ่มมีความกังวลว่าอาจมีความเสี่ยงเกิดขึ้นได้ในอนาคต เนื่องจากการพัฒนาทางเทคโนโลยีอย่างรวดเร็ว และยังเชื่อมโยงกับเทคโนโลยีเกิดใหม่อื่น ๆ ในบางประเทศ ได้เริ่มออกมาตรการเข้มด้านความปลอดภัย ยกตัวอย่าง สหรัฐอเมริกา ที่ได้เริ่มมีแนวทางเกี่ยวกับการใช้ AI ที่ครอบคลุมเรื่อง มาตรฐานใหม่สำหรับความปลอดภัย (AI Safety and Security) การปกป้องความเป็นส่วนตัวของพลเมือง ความเท่าเทียมและสิทธิพลเมือง ส่งเสริมนวัตกรรมและการแข่งขัน รวมถึงหน่วยงานภาครัฐใช้งาน AI ที่ใช้อย่างมีความรับผิดชอบและมีประสิทธิภาพ เช่น

บริษัทด้าน AI ที่มีการพัฒนาและจะส่งผลกระทบต่อความมั่นคงของชาติ เศรษฐกิจ หรือความมั่นคงด้านสุขภาพจะต้องรายงานต่อรัฐบาล กำหนดให้มีการใส่ลายน้ำ (Watermark) สำหรับคอนเทนต์ที่สร้างจาก AI เป็นต้น





# กฎหมายที่เกี่ยวข้อง

## กับความปลอดภัยไซเบอร์ในประเทศไทย

ในประเทศไทยมีกฎหมายเกี่ยวกับความปลอดภัยไซเบอร์ เพื่อควบคุมและป้องกันการกระทำที่ไม่เหมาะสมทางไซเบอร์ รวมถึง การปกป้องข้อมูลส่วนบุคคลและรักษาความมั่นคงของข้อมูล คือ



**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 2560**



โดยมีมาตราที่เกี่ยวข้อง ดังนี้

### มาตรา 9 - 10

แก้ไข ดัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหายโดยมิชอบ  
 คุกไม่เกิน 5 ปี ปรับไม่เกิน 100,000 บาท  
 หรือทั้งจำทั้งปรับ

### มาตรา 11

ส่งข้อมูลหรืออีเมลก่อความรำคาญผู้อื่น หรือการส่งข้อความ  
 ผากร้าย โดยที่ไม่ได้รับอนุญาต

- ส่งโดยปกปิดหรือปลอมแปลงแหล่งที่มา: ปรับไม่เกิน 1 แสนบาท
- ส่งโดยไม่เปิดโอกาสให้ปฏิเสธโดยง่าย: คุกไม่เกิน 2 ปี  
 ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ

### มาตรา 14

การโพสต์ข้อมูลปลอม ทุจริต หลอกลวง ข้อมูลความผิดเกี่ยวกับ  
 ความมั่นคง ข้อมูลลามก หรือ ส่งต่อข้อมูลที่อยู่แล้วว่าผิด

- หากเป็นการกระทำที่ส่งผลถึงประชาชน:  
 ปรับไม่เกิน 4 หมื่นบาท หรือทั้งจำทั้งปรับ
- หากเป็นกรณีที่เป็นการกระทำที่ส่งผลต่อบุคคลใดบุคคลหนึ่ง:  
 โทษจำคุกไม่เกิน 3 ปี ปรับไม่เกิน 6 แสนบาท หรือทั้งจำทั้งปรับ





สิ่งสำคัญเมื่อก้าวสู่การทำงาน  
 ควรเข้าใจบริหารรับความเสี่ยง  
 หากเพเลียงพลาข้อมูลลับสูญหายเกลี้ยง  
 องค์กรเสียชื่อเสียงสูญเงินตรา  
 ก่อนจะเสี่ยงควรป้องกันไม่ประมาท  
 อย่าได้พลาดรู้เท่าทันทุกเวลา  
 ใส่ใจทุกนโยบายล้วนมีค่า  
 ควรรักษาหากภัยมาเตรียมรับมือ

3.1

Behavioral Cyber-Risk Management

ความปลอดภัยเริ่มที่การปกป้อง "ส่วนบุคคล"

- การล่วงละเมิดทางไซเบอร์
- การคุกคามทางไซเบอร์

การล่วงละเมิดทางไซเบอร์ (Cyber Abuse)

รูปแบบการล่วงละเมิดทางไซเบอร์

- การคุกคามทางอิเล็กทรอนิกส์ (Cyberstalking)
- การเปิดเผยข้อมูลส่วนตัว (Doxxing)
- การกลั่นแกล้งทางไซเบอร์ (Cyberbullying)
- การใช้คำพูดเกลียดชัง (Hate Speech)

สาเหตุของการล่วงละเมิดทางไซเบอร์

รับมือการคุกคามทางไซเบอร์

ออนไลน์อย่างไรให้ปลอดภัย?

- สร้างรหัสผ่านที่ยากต่อการทาย
- ใช้การตรวจสอบสิทธิ์ 2 ขั้นตอน
- Passkey

ภัยคุกคามทางไซเบอร์ (Cyber Threat)

รูปแบบภัยคุกคามทางไซเบอร์ในระดับส่วนตัว

- กลยุทธ์ทางวิศวกรรมสังคม
- กลยุทธ์การโจมตีทางเทคนิค

สาเหตุภัยคุกคามทางไซเบอร์

แหล่งข้อมูลเพื่อติดตามสถานการณ์ภัยคุกคามไซเบอร์

# 3.2

## Organizational Cyber-Risk Management

ความเสี่ยงจากการใช้เทคโนโลยีในองค์กร

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

รูปแบบความเสี่ยงไซเบอร์ต่อองค์กร

กลยุทธ์ทางวิศวกรรมสังคม

การโจมตีทางเทคนิค

กฎหมายที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ในประเทศไทย

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 2560

แนวปฏิบัติเพื่อร่วมกันป้องกันภัยไซเบอร์ระดับองค์กร

จัดแบ่งแนวปฏิบัติเป็น 4 กลุ่มใหญ่ ๆ

- ตระหนักระวังภัย
- เกาะติดนโยบาย
- รักรูมด้านเทคนิค
- พร้อมรับหากภัยมา

Update ประเด็นความปลอดภัยทางไซเบอร์ที่ทั่วโลกให้ความสำคัญ

มาตรา 9 - 10 แก้ไข ตัดแปลง หรือทำให้ข้อมูลผู้อื่นเสียหายโดยมิชอบ

มาตรา 11 ส่งข้อมูลหรืออีเมลก่อนผู้อื่นหรือการส่งข้อความฝากร้าน โดยที่ไม่ได้รับอนุญาต

มาตรา 14 การโพสต์ข้อมูลปลอม ทูจจริต หลอกกลาง ข้อมูลความผิดเกี่ยวกับความมั่นคง ข้อมูลลามก หรือส่งต่อข้อมูลที่รู้อยู่แล้วว่าผิด



04



# การสื่อสารดิจิทัล

– Digital Communication –



# แนะนำสำหรับผู้สอน

## • วัตถุประสงค์

ผู้เรียนมีความรู้เกี่ยวกับการสื่อสารในโลกดิจิทัล สิทธิดิจิทัล และปัจจัยที่จะทำให้การสื่อสารหรือการสร้างความร่วมมือสำเร็จ หรือล้มเหลวได้

## • ขอบเขตของเนื้อหา ดังนี้

### 4.1 Digital Footprint Management

- ความหมายและการเกิดขึ้นของ Digital Footprint วันที่สอน  
...../...../.....
- เครื่องมือในการจัดการ Digital Footprint วันที่สอน  
...../...../.....
- ร่องรอยดิจิทัลเชิงบวกและเชิงลบ วันที่สอน  
...../...../.....
- 12 เหตุผลที่ Digital Footprint คือสิ่งสำคัญต่อ HR วันที่สอน  
...../...../.....
- เปิดสถิติ Digital Footprint คือหนึ่งในเหตุผลการรับพนักงานใหม่ วันที่สอน  
...../...../.....

### 4.2 Interaction & Collaboration

- สิ่งที่ทำให้การสื่อสารดิจิทัลประสบความสำเร็จ วันที่สอน  
...../...../.....
- การเลือกใช้เทคโนโลยีเพื่อการสื่อสารอย่างสร้างสรรค์ วันที่สอน  
...../...../.....
- ปัจจัยที่ทำให้การสื่อสารประสบความสำเร็จหรือล้มเหลว วันที่สอน  
...../...../.....
- การรับมือกับประเด็นสื่อสารทางลบ วันที่สอน  
...../...../.....

### 4.3 Future Skill สำหรับการสื่อสาร

- ทักษะสำคัญแห่งยุคดิจิทัล
- มารยาทในโลกดิจิทัล (Netiquette)
- สิ่งควรปฏิบัติในการสื่อสารบนโลกดิจิทัล
- สิ่งที่ควร และไม่ควรทำในโลกดิจิทัล

### 4.4 การกลั่นแกล้งทางไซเบอร์ (Cyberbully)

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

เวลาในการเรียน

# รู้ศัพท์

## ไม่ลับสน



1



### COOKIES

คือ ข้อมูลขนาดเล็กที่ได้มาจากการเชื่อมต่อระหว่างเว็บไซต์ กับเครื่องคอมพิวเตอร์ มีชื่อเต็มยศว่า HTTP COOKIE บ้างก็เรียกว่า เว็บคุกกี้ (WEB COOKIE)

2



### VPN

### เครือข่ายส่วนตัวเสมือน (VIRTUAL PRIVATE NETWORK)

คือ เป็นกลไกสำหรับการสร้างการเชื่อมต่อที่ปลอดภัยระหว่างอุปกรณ์คอมพิวเตอร์กับอินเทอร์เน็ต

3

### CRISIS



### CRISIS MANAGEMENT

คือ กระบวนการที่องค์กรใช้เมื่อประสบเหตุการณ์ที่ไม่คาดคิดมาก่อน เป็นปัญหาที่จำเป็นต้องแก้ไขโดยด่วน เพราะเป็นอันตรายต่อองค์กร พนักงาน และผู้มีผลประโยชน์กับองค์กร

4



### NETIQUETTE

### มารยาทเน็ต จากคำว่า NETWORK ETIQUETTE

คือ กิริยาอาการที่พึงประพฤติปฏิบัติ ในการอยู่ร่วมกันอย่างสันติในสังคมออนไลน์ กล่าวอีกนัยหนึ่งคือ ชุดวิธีประพฤติดนที่เหมาะสม เมื่อคุณใช้อินเทอร์เน็ต

# รู้ศัพท์

## ไม่สับสน



5



### DIGITAL RIGHTS

#### สิทธิดิจิทัล

คือ สิทธิมนุษยชน และสิทธิตามกฎหมาย ที่อนุญาตให้บุคคลเข้าถึง ใช้สร้างและเผยแพร่ สื่อดิจิทัล หรือเข้าถึงและใช้คอมพิวเตอร์อุปกรณ์ อิเล็กทรอนิกส์อื่น ๆ และเครือข่ายโทรคมนาคม

6



### DIGITAL HARASSMENT

คือ การกระทำใด ๆ ในช่องทาง การสื่อสารดิจิทัลที่เกี่ยวข้องกับ เรื่องทางเพศต่อบุคคลอื่นที่เราารู้ได้ว่า ละเมิด ไม่ต้องการ ไม่ยินยอม ไม่พร้อม หรือแม้แต่ยินยอมในขณะนั้น แต่หากส่งผลกระทบต่อผู้ถูกระทำ ถือว่าเป็นการคุกคามทางเพศได้

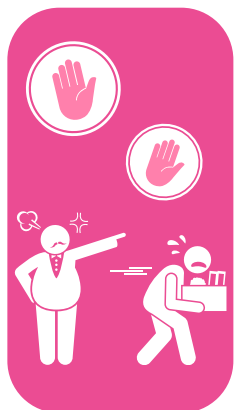
7



### DIGITAL RESILIENCE

#### ภูมิคุ้มกันในโลกดิจิทัล

คือ กระบวนการด้านการปรับตัวทางบวก และลดผลกระทบทางลบต่อชีวิตตนเอง เมื่อต้องเผชิญกับความไม่ปลอดภัย บนโลกออนไลน์



ถ้าคุณเรียนผ่านด้านนี้  
 คุณจะ **ไม่** เสี่ยงถูกไล่ออก  
 เหมือนพนักงานกว่า **34 %**  
 ที่ **ใช้โซเชียลมีเดียไม่เหมาะสม\***

\* 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

1. ผู้เรียนสามารถเข้าใจถึง DIGITAL FOOTPRINT และผลกระทบที่เกิดขึ้น
2. ผู้เรียนสามารถเข้าใจถึงการจัดการและความตระหนักกับ DIGITAL FOOTPRINT ได้

# ร่องรอยการสื่อสาร ที่เราต่างทิ้งไว้



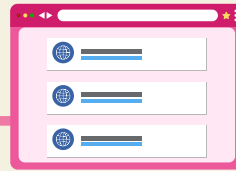
## การสื่อสารดิจิทัล (Digital Communication)

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

และทุกครั้งที่เราสื่อสารผ่านทางดิจิทัล ไม่ว่าจะเป็นการโพสต์ข้อความ แสดงความคิดเห็น แชร์รูปภาพ หรือวิดีโอ ล้วนทิ้งร่องรอยข้อมูลของเราไว้บนโลกออนไลน์ด้วย ซึ่งร่องรอยเหล่านี้เรียกว่า **Digital Footprint**

## Digital Footprint หรือที่เรียกว่า “ร่องรอยดิจิทัล”

หากเปรียบกับการกระทำของเราในโลกความจริงแล้ว ก็เหมือนกับการที่เราไปในสถานที่ต่าง ๆ เมื่อเราเดินผ่านก็จะเกิดรอยเท้า หรือถ้าเดินผ่านใครสักคน ๆ นั้นก็อาจจะจดจำเราได้ 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**



อยากไปเที่ยว



แสดงความเห็น



คัดลอก



แชร์



- **IP Address**

หมายเลขประจำตัว ของอุปกรณ์ที่เราใช้ในการเชื่อมต่ออินเทอร์เน็ต ซึ่งสามารถระบุผู้ให้บริการอินเทอร์เน็ต และตำแหน่งโดยประมาณของเราได้

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

## 2. รอยเท้าดิจิทัลที่เราตั้งใจเผยแพร่ (Active Digital Footprint)

คือร่องรอยข้อมูลที่เราตั้งใจสร้าง 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 และชื่อเสียงของเราในโลกออนไลน์ได้



# เครื่องมือในการจัดการ Digital Footprint

## 1. ตั้งค่าความเป็นส่วนตัวอย่างเข้มงวดบนโซเชียลมีเดีย

รวมทั้งช่องทางทางออนไลน์ต่าง ๆ ที่ใช้งาน และระวังในการแชร์ข้อมูลลงบนโซเชียลมีเดีย

## 2. ลบประวัติการค้นหาและคุกกี้ (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 และส่งผลต่ออัตลักษณ์ดิจิทัลและการทำงานดิจิทัลที่เป็นประโยชน์ด้วย เช่น

- โพสต์อย่างสร้างสรรค์ เป็นกลาง และชื่นชมผู้อื่นด้วยความจริงใจ และมีความระมัดระวังข้อความหรือรูปภาพที่จะทำให้คนผู้นั้นเสียหายได้
- แสดงความคิดเห็นในโพสต์หรือแชตกับผู้อื่น ด้วยข้อความที่สุภาพ นุ่มนวล ไม่ดูถูกความคิดเห็นของผู้อื่น แม้บางครั้งอาจจะมีความเห็นที่ขัดแย้งก็ตาม
- ค้นหาข้อมูลที่เป็นประโยชน์และสร้างสรรค์ ระบบจะเก็บประวัติการค้นหา และอาจมีการนำเสนอเนื้อหาที่เกี่ยวข้องกับเรื่องนั้น ๆ มายังโซเชียลมีเดียที่มีการใช้งานเป็นประจำ เป็นการสะท้อนถึงพฤติกรรมของผู้ใช้งานแต่ละคนไปด้วย

### 2. ร่องรอยดิจิทัลเชิงลบ



เป็นร่องรอยจากพฤติกรรมที่สร้างขึ้น แล้วอาจทำให้ผู้อื่นเดือดร้อนเสียหาย และส่งผลที่ไม่ดีต่ออัตลักษณ์ดิจิทัลของผู้ใช้งาน ไปจนถึงอาจทำให้เกิดโทษหรือสร้างความรำคาญได้ เช่น

- โปสต์พาดพิงถึงผู้อื่นในทางที่ไม่ดี เสียชื่อเสียง หรือไม่ระวัง จนให้เกิดความเสียหายหรืออับอาย
- แสดงความคิดเห็นในโปสต์ของผู้อื่นด้วยข้อความที่ไม่สุภาพ หยาดคาย หรือถ้อยคำที่รุนแรง หรือสร้างความขัดแย้ง อาจทำให้เกิดการตอบโต้ หรือโต้เถียงกัน
- ค้นหาข้อมูลที่ไม่เป็นประโยชน์หรือข้อมูลที่ไม่สร้างสรรค์ เช่น การค้นหาข้อมูลเกี่ยวกับความรุนแรง เรื่องเพศ หรือข้อมูลการพนัน ซึ่งเมื่อค้นหาข้อมูลที่ไม่สร้างสรรค์เหล่านี้บ่อยครั้ง ระบบจะเก็บข้อมูลและนำเสนอข้อมูลในลักษณะเดียวกัน แม้ว่าภายหลังเราจะไม่ได้ค้นหาหรือพูดถึงมันแล้วก็ตาม เราจะติดอยู่ใน “ฟองสบู่ข่าวสาร” (Filter Bubble) รับสารด้านเดียว จนเกิดเป็นความเชื่อผิด ๆ ได้ และบางครั้งอาจทำให้เราวางตัวเองเป็นศูนย์กลางของทุกอย่าง หรือถ้ารับความเห็นด้านลบมามาก ๆ ก็มีโอกาที่จะตกอยู่ในความสิ้นหวังได้ด้วย

ผลกระทบในเชิงลบที่เกิดขึ้น อาจจะเป็นการละเมิดสิทธิผู้อื่น ถึงขั้นการฟ้องร้องทางกฎหมาย หรือมีผลกับการเรียนและการทำงานในอนาคต โดยร่องรอยดิจิทัลที่สร้างขึ้น สามารถที่จะนำไปเป็นหลักฐานในทางกฎหมายได้

สุดท้ายหากร่องรอยดิจิทัลของเราดูแล้วมีปัญหา มีแต่แง่ลบ ทำตัวไม่ดี ก็สามารทำให้ HR ที่เข้ามาตรวจเช็คโซเชียลมีเดียช่วงที่สมัครงานตัดสินใจไม่จ้างงานเราได้



# 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 เริ่มนำมาเป็นส่วนหนึ่งในการตัดสินใจคัดเลือกพนักงานมากขึ้น และในขณะเดียวกัน ผู้สมัครงานก็สามารถตรวจสอบ Digital Footprint ของบริษัทที่กำลังจะสมัครงานได้ด้วย โดย **Forbes (นิตยสารเกี่ยวกับธุรกิจและการเงินในสหรัฐอเมริกา)** ได้กล่าวถึงเหตุผล 12 ข้อที่ Digital Footprint สำคัญต่อ HR ดังนี้

## 1 ข้อมูลออนไลน์สามารถบ่งบอกถึงความเหมาะสมต่อบริษัท

การจ้างงานมีผลต่อความสำเร็จขององค์กร การศึกษาข้อมูลออนไลน์ของผู้สมัคร จะทำให้ทราบคร่าว ๆ ว่า เขาเหมาะสมกับเป้าหมายขององค์กรหรือไม่



## 2 แสดงให้เห็นตัวตนอีกด้านของผู้สมัคร

การมีตัวตนในโลกออนไลน์ที่โดดเด่น น่าสนใจ ก็จะสร้างความแตกต่างท่ามกลางตัวเลือกมากมายได้



## 3 กำจัดผู้สมัครที่อาจมีปัญหาวออกไป

เราสามารถเห็นพฤติกรรมทั้งดีและไม่ดีในโลกออนไลน์ โดยสามารถนำข้อมูลเหล่านั้นมาประเมินว่าจะส่งผลอย่างไรกับบริษัทบ้าง



## 4 ดูว่าการแสดงตัวตนทางออนไลน์ของผู้สมัคร

มีคุณค่ากับองค์กรหรือไม่



## 5 ข้อมูลออนไลน์ทำให้มองเห็นผู้สมัคร 360 องศา

เพื่อประเมินทักษะ ความสามารถ และตัวตนของผู้สมัครว่าสอดคล้องกับวัฒนธรรมองค์กรหรือไม่



## 6 กบวณผิดพลาด หรืออคติที่ได้รับมา

บางครั้งเราได้รับผิดพลาดที่ไม่ดีของผู้สมัครมา การเข้าไปตรวจสอบข้อมูลดิจิทัลก็จะช่วยให้เราทบทวนและประเมินอคตินั้น ๆ ว่าเป็นจริงหรือไม่



## 7 สามารถประเมินบุคลิกภาพเบื้องต้น

ท่ามกลางสถานการณ์ COVID-19 ที่เผชิญหน้ากันโดยตรงอาจเป็นเรื่องยาก การเข้าไปตรวจสอบข้อมูลออนไลน์ก็จะช่วยให้ HR เห็นบุคลิกและทัศนคติคร่าว ๆ ของผู้สมัครง่ายขึ้น



## 8 ตรวจสอบความสนใจ ว่าสอดคล้องกับบริษัทหรือไม่

ทุกวันนี้ผู้สมัครหลายคนมีบล็อกเป็นของตัวเอง หรือเราสามารถเช็คดูการมีส่วนร่วมของเขาว่าอยู่ในกลุ่มความสนใจใด เช่น เราเป็นบริษัทขายเสื้อผ้า และผู้สมัครเขียนบล็อกเกี่ยวกับแฟชั่น ก็จะส่งผลดีต่อธุรกิจของเราได้



## 9 เห็นผู้สมัครในฐานะคนคนหนึ่ง

การตรวจสอบข้อมูลออนไลน์ก็จะเห็นทักษะอื่นด้วย เช่น ทักษะการสื่อสาร การเป็นผู้นำ การตัดสินใจ



## 10 ตัวตนทางดิจิทัลจะบ่งบอกว่า อะไรสำคัญต่อผู้สมัคร

ไม่ว่าจะเป็นบล็อกที่เขียน บทความที่แชร์ หรือ LinkedIn เป็นเครื่องมือสำคัญในการประเมินตัวผู้สมัคร เพราะจะสะท้อนว่าอะไรอยู่ในความสนใจ มีรสนิยมอย่างไร และมีไลฟ์สไตล์อย่างไร



## 11 สร้างความชัดเจนจากการสัมภาษณ์

บางครั้งการสัมภาษณ์อาจไม่เพียงพอ การตรวจสอบเช็คข้อมูลออนไลน์ก็จะทำให้เรื่องราวเหล่านั้นกระจ่างชัดเจนมากขึ้น



## 12 เป็นสิ่งที่ควรทำ และหลีกเลี่ยงความประหลาดใจ

หลายคนชอบโพสต์โซเชียลมีเดียทุกวัน ซึ่งจะบ่งบอกว่า เขามองโลก หรือมีความคิดเห็นอย่างไร และนั่นเป็นสิ่งที่นายจ้างควรรู้



# เปิดสถิติ 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 โดยสิ่งที่คุณเขาตรวจสอบก็คือ

คุณสมบัติสนับสนุนในการจ้างงาน 58%



ความเป็นมืออาชีพในโลกออนไลน์ 50%



สิ่งที่คนอื่นโพสต์เกี่ยวกับผู้สมัคร 34%



เหตุผลที่จะไม่รับผู้สมัคร 22%



### 3 อันดับ Digital Footprint ร้ายแรงที่จะไม่รับเข้าทำงาน



อันดับที่ 1 โพสต์ภาพ วิดีโอ หรือข้อมูลยั่วหรือไม่เหมาะสม 40%

อันดับที่ 2 โพสต์ภาพการดื่มสุราหรือใช้ยาเสพติด 36%

อันดับที่ 3 โพสต์ข้อความเหยียดเพศ เชื้อชาติ ศาสนา 31%

### 3 อันดับ Digital Footprint ที่เป็นประโยชน์ต่อการรับเข้าทำงาน



อันดับที่ 1 ประวัติผู้สมัครสนับสนุนต่อหน้าที่การงาน 37%

อันดับที่ 2 มีความคิดสร้างสรรค์ 34%

อันดับที่ 3 ตัวตนออนไลน์มีความเป็นมืออาชีพ 33%

## EXAMPLE

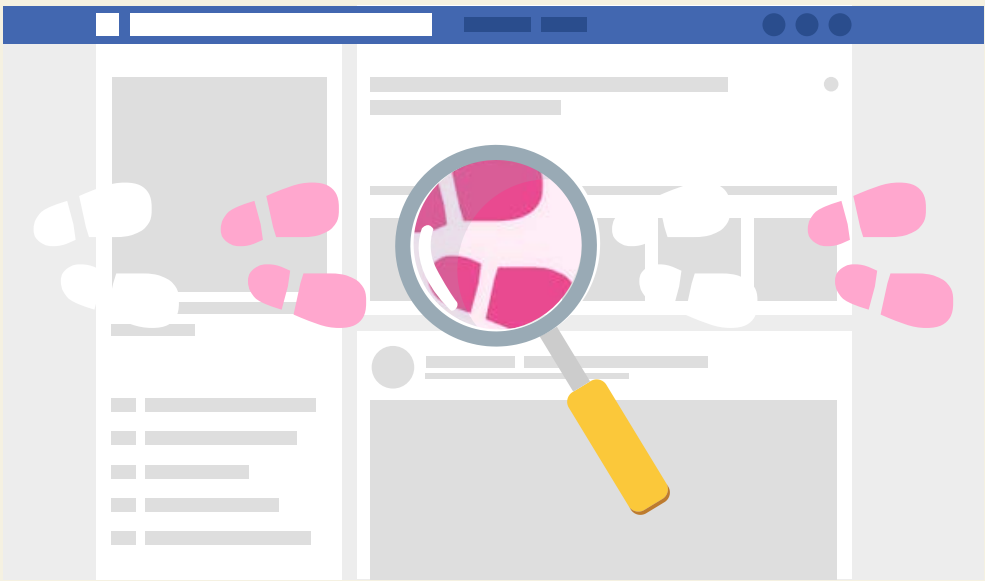
## ยกตัวอย่างจากข่าวเรื่อง รอยเท้าดิจิทัล : ฝ่ายบุคคลเตือน ตัวตนและความคิดเห็น ในโลกออนไลน์มีผลต่อการสมัครงาน



ดร.บวรนนท์ ทองกล้า นายกสสมาคมการจัดการงานบุคคลแห่งประเทศไทย เปิดเผยกับบีบีซีไทยว่า ปัจจุบันองค์กรธุรกิจจำนวนมากใช้ข้อมูลจากโซเชียลมีเดียประกอบการพิจารณารับสมัครคนเข้าทำงาน นอกเหนือจากการสัมภาษณ์ และการทดสอบความสามารถ ดังนั้น คนในตลาดแรงงานจึงควรระมัดระวังในการเปิดเผยข้อมูลส่วนตัว และความคิดเห็นในโลกออนไลน์ เพราะอาจส่งผลกระทบต่อการสมัครงาน

"โซเชียลมีเดียเหล่านี้เก็บข้อมูลของบุคคลได้ทั้งหมด ทำให้ฝ่ายบุคคลวิเคราะห์ผู้สมัครได้ง่าย และได้ผลมากกว่าการนั่งสัมภาษณ์แบบเดิม ๆ เพราะเราจะรู้ได้ว่าเขาให้ความสำคัญกับเรื่องไหนในชีวิต ทัศนคติ วิธีป่วน วิธีคิด" ดร.บวรนนท์กล่าว

แนวโน้มนี้ได้รับการยืนยัน จากการสำรวจของสมาคมการจัดการงานบุคคลฯ เรื่องกระบวนการรับสมัครงานของบริษัทเอกชน 350 แห่ง ซึ่งจัดทำเมื่อเดือนมิถุนายนปี 2019 ผลการสำรวจพบว่า 41.19 เปอร์เซ็นต์ขององค์กรที่สำรวจ ดูโซเชียลมีเดียของผู้สมัครประกอบการพิจารณาคุณสมบัติเพื่อตัดสินใจรับเข้าทำงาน





การสื่อสารข้อมูลดิจิทัล  
 ล้วนทิ้งร่องรอยนั้นไว้มีจางหาย  
 สร้างรอยเท้าคนจดจำเรามากมาย  
 โพสต์หลากหลายแชร์ส่งทุกช่องทาง  
 เปรียบตั้งเป็นประวัติผลสองด้าน  
 ทุกข์แผ้วพานหรือมีสุขอยู่ที่สร้าง  
 ประวัติไหนที่ไม่ดีให้ลบล้าง  
 ตั้งค่าอย่างเข้มงวดเป็นส่วนตัว



ถ้าคุณเรียนผ่านด้านนี้  
คุณจะมี ทักษะการสื่อสารที่ดีขึ้น  
ซึ่งถือเป็น ทักษะสำคัญอันดับ 1  
ที่นายจ้างกำลังมองหา

อ้างอิงข้อมูลจาก

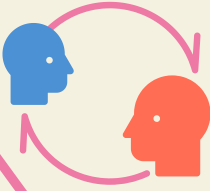
<https://www.blockdit.com/posts/66544213f864a30fba993157>

# 4.2

## INTERACTION & COLLABORATION

### วัตถุประสงค์

1. ผู้เรียนสามารถเลือกใช้วิธีการสื่อสารที่เหมาะสมได้
2. ผู้เรียนสามารถวิเคราะห์ปัจจัยที่จะทำให้การสื่อสารหรือการสร้างความร่วมมือสำเร็จ หรือล้มเหลวได้



# ทักษะพื้นฐาน สื่อสารอย่างเข้าใจ

การสื่อสารเป็นทักษะพื้นฐานสำคัญอย่างหนึ่งในการทำงาน และการดำรงชีวิต หากเรามีการสื่อสารที่สร้างสรรค์จะช่วยให้ เกิดความเข้าใจซึ่งกันและกัน ลดความขัดแย้ง มีการแลกเปลี่ยนความรู้ และทำให้การร่วมมือกันทำงานนั้นมีประสิทธิภาพ

## สิ่งที่ทำให้การสื่อสารดิจิทัล ประสบความสำเร็จ

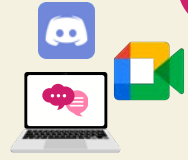


เกิดจากปัจจัยหลายประการ เช่น

- ความสะดวกรวดเร็ว
- การเข้าถึงคนจำนวนมากผ่านการโพสต์หรือแชร์ข้อมูลผ่านแพลตฟอร์มที่ได้รับความนิยม
- การรองรับเนื้อหาในรูปแบบที่หลากหลายตามเทคโนโลยีที่ใช้งาน
- สามารถทำได้โดยไม่จำกัดสถานที่ และมีต้นทุนต่ำ

# การเลือกใช้เทคโนโลยี

## เพื่อการสื่อสารอย่างสร้างสรรค์



การเลือกใช้เทคโนโลยีเพื่อการสื่อสารให้เหมาะสมกับกลุ่มเป้าหมาย ที่จะสื่อสารจะเป็นสิ่งที่ต้องคิดคำนึงถึงเป็นอันดับต้น ๆ เราอาจต้องเริ่มจากพิจารณาจากความเหมาะสมของคนหรือกลุ่มคนที่เราจะมีปฏิสัมพันธ์ด้วย

### 1. การสื่อสารระหว่างบุคคล

เลือกใช้สื่อเทคโนโลยีที่เหมาะสมกับการสื่อสารแบบตัวต่อตัว และไม่มีผู้อื่นเข้ามาแทรก เช่น โทรศัพท์ หรือ การสนทนาผ่านช่องทางส่วนตัว

### 2. การสื่อสารระหว่างกลุ่มคน เฉพาะกลุ่มแบบไม่เป็นสาธารณะ

อาจใช้วิธีการตั้งกลุ่มการสื่อสาร ที่อนุญาตเฉพาะผู้ที่มีส่วนเกี่ยวข้องถึงจะเข้าร่วมได้

### 3. การสื่อสารระหว่างกลุ่มคนแบบเป็นสาธารณะ

ใช้การโพสต์เป็นสาธารณะหรือตั้งกลุ่ม ซึ่งคนที่มีความสนใจสามารถเข้าร่วมกลุ่มได้อย่างอิสระ โดยไม่ต้องรอถูกเชิญเข้ากลุ่ม แต่ต้องปฏิบัติตามข้อกำหนดของกลุ่ม

# ปัจจัยที่ทำให้การสื่อสาร

## ✓ ประสบความสำเร็จหรือล้มเหลว ✗

### 1. เครื่องมือสื่อสารดีมีชัยไปกว่าครึ่ง



เลือกเครื่องมือสื่อสารให้เหมาะสมกับเป้าหมายที่ต้องการสื่อสาร โดยต้องคิดถึงข้อจำกัดต่าง ๆ เช่น ปัญหาอินเทอร์เน็ต ไม่ค่อยดี หรือมีสัญญาณรบกวน รวมถึงทักษะการใช้เครื่องมือ หรือความคุ้นเคยกับช่องทางที่ใช้ทั้งในฝั่งผู้ส่งและผู้รับสาร

### 2. เนื้อหาชัดเจน สื่อสารจับใจ



เนื้อหาที่สื่อสาร ต้องบอกเล่าความต้องการของผู้ส่งได้ ไม่คลุมเครือ ไม่สร้างความขัดแย้ง มีที่มาที่ไป

### 3. เข้าใจความต่าง หนทางของผู้อยู่เป็น



เข้าใจในวัฒนธรรมและการใช้ภาษาที่แตกต่างกัน เนื่องจากเราอยู่กันคนละที่ บางคนอาจไม่เคยพบเจอกันในโลกแห่งความเป็นจริง

#### 4. ภาพจำดี มีมารยาท



รักษามารยาท

ควรมีมารยาทในการสื่อสาร ยิ่งถ้ามีการประชุมออนไลน์ให้พยายามรักษามารยาทเหมือนการประชุมจริง ๆ ตัวอย่างเช่น เข้าประชุมตรงเวลา แต่งตัวให้เรียบร้อย เปิดกล้องและเปิดฟังก์ชันเบลอพื้นหลัง กดปุ่มยกมือก่อนพูดหรือเสนอความคิดเห็น รวมไปถึง การทำสภาพแวดล้อมให้เหมาะสมกับการประชุม เช่น มีแสงที่เพียงพอ หรือแยกสัตว์เลี้ยงไปไว้อีกที่หนึ่ง

#### 5. วิเคราะห์สรุปเจียบ เปรียบพร้อมด้วยแนวทาง



วิเคราะห์ และปรับแนวทางการสื่อสารให้เหมาะกับทัศนคติ ประสบการณ์ และความเชื่อของกลุ่มเป้าหมาย เพราะผู้คนใช้สิ่งเหล่านี้ ตีความเนื้อหาที่ได้รับรู้มาแตกต่างกันไป

#### 6. สื่อสารอย่างเข้าใจ ตีต่อใจคุณผู้ฟัง



ผู้ส่งสารต้องเข้าใจในสิ่งที่ต้องการสื่อสารเป็นอย่างดี มีเจตนาที่ดีและเคารพผู้ฟัง

#### 7. รับสารอย่างดี เพิ่มดีกรีความเข้าใจ



ผู้รับสารต้องพยายามทำความเข้าใจและตั้งใจรับฟังเนื้อหา

# การรับมือกับ

# ประเด็นสื่อสารทางลบ

## ระดับบุคคล

1. หลีกเลี่ยงการโต้ตอบทันที  
ที่เห็นข้อความเชิงลบ



2. ถอยออกมาประเมินสถานการณ์ให้ดีกว่าก่อนตอบ  
พิจารณาว่ามีพื้นฐานความจริงหรือไม่ บางครั้ง  
อาจเลือกที่จะไม่ตอบโต้หากไม่มีประโยชน์

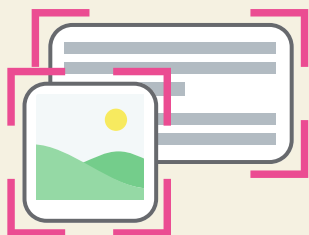
3. ใช้การตั้งค่าความเป็นส่วนตัว  
ตามความเหมาะสมของข้อมูล



4. หากมีสถานการณ์ด้านลบเกิดขึ้น  
ให้ปรึกษาหรือระบายกับคนที่ไว้ใจได้

5. กดรายงาน หรือบล็อกทันที หากถูก  
คุกคาม จนเกินขอบเขตที่ยอมรับได้

รายงาน



6. หากถูกคุกคามให้ทำการบันทึกหลักฐาน หรือ  
แคปรูปภาพ เพื่อเป็นหลักฐานในการดำเนินการ  
ทางกฎหมาย

7. ดูแลสุขภาพจิต หากสถานการณ์ด้านลบมี  
ผลกระทบต่อจิตใจอย่างมาก ให้ปรึกษาผู้  
เชี่ยวชาญด้านจิตวิทยา



8. ใช้ประสบการณ์ต่าง ๆ ที่ได้รับไปพัฒนา  
ปรับปรุงทักษะการสื่อสารบนโลกดิจิทัล

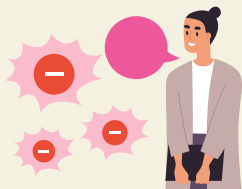
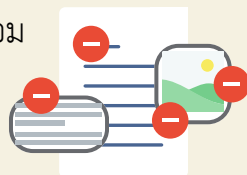
# การรับมือกับ



# ประเด็นสื่อสารทางลบ

## ระดับองค์กร

1. เตรียมพร้อมรับมือการสื่อสารทางลบ ที่มักเกิดขึ้นได้  
เสมอในองค์กร สร้างการตระหนักรู้และการเตรียมพร้อม  
โดยการทำความเข้าใจเกี่ยวกับภัยคุกคามทางดิจิทัล  
และควรมีนโยบาย หรือแนวทางการจัดการที่ชัดเจน



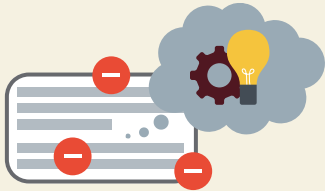
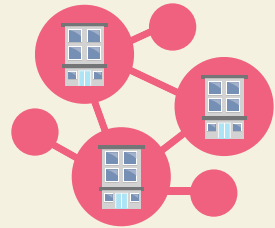
2. ตอบสนองอย่างมืออาชีพ  
มีเหตุผลและหลีกเลี่ยงการใช้อารมณ์

3. มีแผนการจัดการวิกฤต และจัดตั้งทีมไว้  
สำหรับจัดการสถานการณ์วิกฤต เพื่อรับมือ  
และรักษาภาพลักษณ์ขององค์กร  
ในสถานการณ์ฉุกเฉิน



4. การสื่อสารที่ตรงไปตรงมา  
และเป็นความจริง

5. การมีเครือข่ายพันธมิตร จะช่วยเหลือนับสนุนองค์กรในการจัดการสถานการณ์ต่าง ๆ ได้

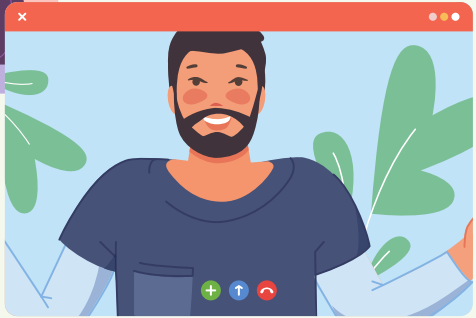


6. ติดตามและวิเคราะห์สถานการณ์ด้านลบที่เกิดขึ้นอย่างใกล้ชิด เพื่อหาวิธีการตอบสนองที่ดีที่สุด และมีผลกระทบน้อยที่สุด

7. ศึกษา และอบรมกระบวนการเกี่ยวกับการสื่อสารดิจิทัลที่มีประสิทธิภาพ เช่น Crisis Management

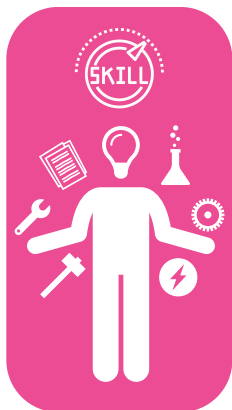


8. กำหนดแผนองคฺกร โดยให้ความสำคัญกับสุขภาพจิตของบุคคลในองคฺกร





ทักษะหนึ่งสำคัญขั้นพื้นฐาน  
คือสื่อสารอย่างสร้างสรรค์และเข้าใจ  
คำนึงถึงสื่อเทคโนโลยีที่เลือกใช้  
ควรเลือกให้เหมาะสมกับบุคคล  
ปัจจัยที่การสื่อสารจะสำเร็จ  
ควรถือเคล็ดเครื่องมือดีบังเกิดผล  
เนื้อหาชัดเจนวิเคราะห์เฉียบเข้าถึงคน  
จะรอดพ้นความล้มเหลวได้ด้วยดี



ถ้าคุณเรียนผ่านด้านนี้ คุณจะมี  
 ทักษะแห่งอนาคตเพิ่มขึ้น  
 เป็นทักษะที่ นายจ้างกว่า 75%  
 มองว่า สำคัญมากในอนาคต\*

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

อ้างอิงข้อมูลจาก

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

## 4.3

# FUTURE SKILL

## สำหรับการสื่อสาร

### วัตถุประสงค์

1. ผู้เรียนมีความรู้เกี่ยวกับ มารยาทในโลกดิจิทัล (NETIQUETTE) และแนวทางปฏิบัติในการส่งข้อความหรือโพสต์เพื่อสื่อสารบนโลกดิจิทัล



# ทักษะสำคัญ แห่งยุคดิจิทัล



## Future Skill สำหรับการสื่อสาร เป็นทักษะสำคัญสำหรับยุคปัจจุบัน

ทักษะนี้มีส่วนสำคัญอย่างมากในการทำงานร่วมกับคนอื่น และสามารถทำงานได้อย่างมีประสิทธิภาพเพิ่มมากขึ้น จึงขอแนะนำทักษะที่น่าศึกษาหรือฝึกฝนก่อนเริ่มทำงาน 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 การรู้เท่าทันความปลอดภัยในโลกไซเบอร์ (Cybersecurity Awareness)

ความรู้ และความตระหนักเกี่ยวกับภัยคุกคามในโลกดิจิทัล และการปกป้อง ข้อมูลส่วนบุคคล และข้อมูลขององค์กร

## 6 ทักษะการสื่อสารข้ามวัฒนธรรม (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)

ความสามารถในการคิดนอกกรอบ สร้างสรรค์แนวคิดใหม่ๆ และหาทางออกที่ไม่เหมือนใคร

## 10 การทำงานร่วมกัน (Collaboration)

ความสามารถในการทำงานร่วมกับผู้อื่นอย่างมีประสิทธิภาพ แบ่งปันความคิดเห็น และแก้ไขปัญหาไปด้วยกัน

## 11 ภาวะผู้นำ (Leadership)

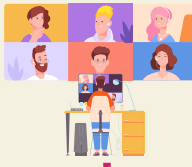
ความสามารถในการนำทีม สร้างแรงบันดาลใจ และผลักดันให้ทีมงานบรรลุเป้าหมายร่วมกัน

## 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 เช่นเดียวกับที่เราต้องการได้รับการปฏิบัติ ไม่เหยียดหยามใคร

### 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. เป็นผู้ฟังที่ดี

เปิดใจรับฟังความคิดเห็นของผู้อื่น เคารพในความแตกต่าง

#### 10. สนุกกับโลกออนไลน์

ใช้เทคโนโลยีอย่างสร้างสรรค์ แบ่งปันสิ่งดี ๆ สร้างมิตรภาพ

# สิ่งที่ควรปฏิบัติ ในการสื่อสารบนโลกดิจิทัล

## 1. ใช้ข้อความที่ชัดเจนและกระชับ เข้าใจได้ง่าย

หลีกเลี่ยงการใช้ภาษาที่คลุมเครือ

## 2. หลีกเลี่ยงการใช้ภาษาที่ไม่เหมาะสม ไม่สุภาพ

คำที่มีลักษณะล่วงละเมิด หรือคำแสลงที่อาจทำให้ผู้รับสารเข้าใจผิด

## 3. เคารพความเป็นส่วนตัวของผู้อื่น

ไม่ส่งต่อข้อมูลส่วนตัวหรือข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต

## 4. ตรวจสอบข้อความ และการสะกดคำก่อนส่งทุกครั้ง

เพื่อป้องกันข้อผิดพลาดและการเข้าใจผิด

## 5. ให้ความสำคัญกับการตอบกลับข้อความในเวลาที่เหมาะสม

หลีกเลี่ยงการทิ้งข้อความที่ต้องการการตอบกลับเป็นเวลานาน

## 6. Emoji ควรใช้ให้พอเหมาะ และเหมาะสม

จะช่วยแสดงความรู้สึกและทำให้ดูมีชีวิตชีวา แต่ ต้องใช้ให้พอเหมาะ และดูบริบทให้เหมาะสมด้วย

## 7. เคารพในความหลากหลาย

ของแต่ละวัฒนธรรมและบุคคล หลีกเลี่ยงการใช้คำ หรือข้อความที่อาจถูกตีความว่าเป็นการเลือกปฏิบัติหรือไม่เคารพ

# สิ่งที่ควร และไม่ควรทำ

## ในโลกดิจิทัล



ถ้าเราอยากฝึกมารยาทในโลกดิจิทัลให้เริ่มจากการเรียนรู้สิ่งที่ควร และไม่ควรทำในโลกดิจิทัล ดังนี้

### 1. สิ่งที่ต้องทำ



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

### 2. สิ่งที่ไม่ควรทำ



- แสดงความคิดเห็นด้วยถ้อยคำที่รุนแรง
- แสดงอารมณ์ขันที่หมิ่นเหม่ เสียตสี
- ส่งต่อข้อมูลที่เราไม่แน่ใจว่าเป็นความจริงหรือไม่
- ใช้โซเชียลมีเดียในการให้ร้ายผู้อื่น



# มารยาทในการประชุมออนไลน์

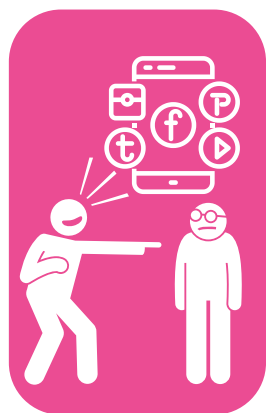
ปัจจุบันเนื่องจากเกิดการเปลี่ยนแปลงรูปแบบการทำงาน ทำให้การประชุมหรือการเรียนออนไลน์นั้น มีบทบาทในชีวิตของเรามากขึ้น สิ่งที่ไม่ควรลืมเลยคือ มารยาทในการประชุมออนไลน์ โดยมีวิธีปฏิบัติต่างๆ ดังนี้

1. เข้าประชุมตรงต่อเวลา
2. ปิดกล้อง และเปิดฟังก์ชันเบลล์ฟอน์หลัง เพราะบางครั้งฉากด้านหลังของเราอาจไม่เรียบร้อย ซึ่งอาจจะส่งผลเสียต่อภาพลักษณ์หรือรบกวนการประชุมได้
3. แต่งตัวให้เรียบร้อย แม้การประชุมออนไลน์จะเห็นเพียงร่างกายส่วนบนก็ควรจะต้องจัดแต่งทรงผมให้เรียบร้อย เพื่อแสดงความพร้อม และความตั้งใจ
4. กดปุ่มยกมือก่อนพูด หรือเสนอความคิดเห็นทุกครั้ง
5. พยายามทำสภาพแวดล้อมให้เหมาะสมกับการประชุม เช่น หากคุณมีสัตว์เลี้ยงให้แยกออกไปอยู่อีกห้องหนึ่ง หรือไม่นั่งในที่ที่แสงมีตจนเกินไป





เสริมทักษะสำคัญประจำยุค  
 ไม่กระตุกการทำงานสัมฤทธิ์ผล  
 คิดสร้างสรรค์แก้ปัญหาไร้กังวล  
 ปรับตัวตนสร้างสัมพันธ์ผู้นำดี  
 และอีกสิ่งที่สำคัญขาดไม่ได้  
 มารยาทเสริมไมตรีเป็นเกียรติศรี  
 คิดก่อนพูดรู้จักคอยรับฟังดี  
 ใช้พาทีสุภาพสร้างมิตรเอื้อ



ถ้าคุณเรียนผ่านด้านนี้  
คุณจะมีส่วนช่วยหยุดวงจร  
การกลั่นแกล้งบนโซเชียล  
และไม่เสี่ยงทำผิดกฎหมาย  
ที่มีโทษสูงทั้งจำและปรับ

อ้างอิงข้อมูลจาก

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

# 4.4

## CYBERBULLY

### วัตถุประสงค์

1. ผู้เรียนมีความรู้เกี่ยวกับ CYBERBULLY ได้
2. ผู้เรียนสามารถเข้าใจถึงสิทธิดิจิทัลได้

# การสื่อสาร เครื่องมือสำคัญ ในการปกป้องสิทธิดิจิทัล



การสื่อสารทางดิจิทัล มีความสำคัญอย่างมากในยุคนี้ เพราะช่วยให้การสื่อสารเกิดขึ้นได้อย่างสะดวก รวดเร็ว และมีประสิทธิภาพ ไม่ว่าจะในด้านธุรกิจ กระบวนการทำงาน การศึกษา การใช้ชีวิตประจำวัน ช่วยให้ผู้คนสามารถเชื่อมต่อกันได้ไม่ว่าจะอยู่ที่ใดบนโลก ส่งผลให้เกิดการแลกเปลี่ยนข้อมูล ความคิดเห็น วัฒนธรรมที่หลากหลาย อีกทั้งยังเป็น **เครื่องมือสำคัญ** ในการสร้างความตระหนักรู้เกี่ยวกับสิทธิดิจิทัล และส่งเสริมให้ผู้คนเข้าใจ และปกป้องสิทธิของตนเอง

## สิทธิดิจิทัล หรือ Digital Rights



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

# "คนทำไม่เคยจดจำ แต่ผู้ถูกกระทำกลับไม่เคยลืม"



Cyberbully (การกลั่นแกล้งทางไซเบอร์)

จบอยู่แค่ช่วงเวลาวัยรุ่น จริงหรือ ?

ปัจจุบัน การกลั่นแกล้งทางไซเบอร์ เป็นปัญหาใหญ่ที่มีอยู่ทุกที่บนโลกออนไลน์ แม้กระทั่งสังคมการทำงาน การโดนการกลั่นแกล้งทางไซเบอร์ก็ยังคงมีอยู่อย่างมากมาย ซึ่งมักจะมีเรื่องของการเมืองในที่ทำงานเข้ามาเกี่ยวข้อง ทำให้ทุกคนมีโอกาสที่จะเจอการ การกลั่นแกล้งทางไซเบอร์ทั้งนั้น ในไทยปัญหาการละเมิดสิทธิดิจิทัลที่เป็นเรื่องใหญ่อันดับต้น ๆ นั้น คือ การกลั่นแกล้งทางไซเบอร์

## การกลั่นแกล้งทางไซเบอร์ (Cyberbully) ใคร ๆ เขาก็ทำกัน... จริงหรือ ?

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

### 1. การปะทะคารม (Flaming)

คือ การโต้เถียงไปมาระหว่างบุคคล จนก่อให้เกิดความรุนแรง มีการใช้ถ้อยคำที่ก้าวร้าว และมีการดูถูกเหยียดหยาม มักเกิดขึ้นในพื้นที่สาธารณะ (เช่น ตามกระทู้บอร์ดสนทนา) มากกว่าพื้นที่ส่วนตัว (เช่น อีเมล)

## 2. การก่อกวน (Harassment)

คือ การใช้ถ้อยคำหรือการกระทำใดๆ ที่สร้างความรำคาญใจและความทุกข์ใจต่อบุคคลหนึ่งโดยเจตนา โดยกระทำซ้ำ ๆ ส่วนใหญ่จะเกิดขึ้นในพื้นที่ส่วนตัว เช่น ช่องสนทนาทาง Facebook

## 3. การใส่ร้ายป้ายสี (Denigration)

คือการส่งต่อข้อมูลของบุคคลที่ไม่เป็นความจริง ผู้ส่งอาจนำข้อมูลไปเผยแพร่ในพื้นที่สาธารณะตามเว็บไซต์ต่าง ๆ รวมไปถึงพื้นที่ส่วนตัว

## 4. การปลอมตัวเป็นบุคคลอื่น (Impersonation)

การแอบอ้างเป็นบุคคลหนึ่ง และกระทำการที่สร้างความเสียหายให้กับบุคคลนั้น เช่น ใช้ถ้อยคำหยาบคายด่าว่ากล่าวผู้อื่น เผยแพร่ข้อมูลที่ไม่เหมาะสมให้กับผู้อื่น ช่มเหงรังแกบุคคลอื่น เป็นต้น

การปลอมตัวเป็นบุคคลอื่น สามารถทำได้โดยการสร้างตัวตนเลียนแบบบุคคลนั้นขึ้นมาใหม่ หรือขโมยรหัสผ่านของบุคคลนั้นเพื่อใช้ตัวตนบนโลกออนไลน์ของบุคคลนั้นทำสิ่งที่ไม่เหมาะสม

## 5. การถ่ายคลิปวิดีโอและนำไปเผยแพร่ลงบน อินเทอร์เน็ต (Video Recording of Assaults)

คือ การนำคลิปวิดีโอไปเผยแพร่ตามที่ต่าง ๆ บนอินเทอร์เน็ต เพื่อสร้างความอับอายให้กับคุณนั้น

## 6. การส่งสิ่งที่มีความล่อแหลมทางเพศ (Sexting)

คือ การส่งข้อความ รูปเปลือย หรือรูปกึ่งเปลือยที่มีความล่อแหลมทางเพศให้กับผู้อื่น

บางครั้ง ก็เพิ่มความเสี่ยงของการกลั่นแกล้ง ด้วยการพูดถึงประเด็นของคนที่ถูกบูลลี่ เพราะเห็นว่าใคร ๆ ก็ทำกัน ทั้งที่การกลั่นแกล้งบนโลกออนไลน์แทบทุกครั้งเกิดจากความตั้งใจ แต่บางคนก็ใช้ข้ออ้างว่า “อีกฝ่ายอ่อนแอเอง” มาเป็นข้ออ้างลดความรู้สึกผิดในจิตใจ

## อ่อนแอก็แพ้อะไร

เป็นวลีที่บ่งชี้ว่าปัจจุบันหลายคนมองว่าทุกอย่างคือ การแข่งขัน ต้องการเอาชนะ ต้องการเป็นที่สนใจ ใครที่ไม่ไหวก็ยอมแพ้อะไรซะ อาจจะได้ความได้ว่าบางครั้งสาเหตุหลักของการกลั่นแกล้งทางไซเบอร์นี้ คือการที่ไม่ต้องการให้ใครโดดเด่นกว่าตัวเอง

## ทำไมบางคนไม่ตระหนักถึง ความรุนแรงของการกลั่นแกล้ง ทั้งที่มันทำร้าย และคร่าชีวิตคนได้ ?

ส่วนหนึ่งน่าจะเป็นเพราะความรู้สึกไม่ชอบใจคนที่ตัวเองแกล้ง และอาจเพราะรู้สึกว่าการกลั่นแกล้งในโลกออนไลน์ไหลลื่นเข้ามา เป็นประเด็นดราม่า แล้วซั๊กพั๊กก็ผ่านไป พอถึงช่วงหนึ่งทุกคนก็พากันลืมหมด แต่เราอาจจะลืมไปว่า... รอยแผลเป็นบางครั้งก็ยากที่จะลบเลือน เช่นเดียวกับคนที่โดนก็ยากที่จะลืม อาจจะพูดติดตลกว่า เดียวนี้รอยแผลเป็นเราก็ใช้เทคโนโลยีลบออกได้ แต่ทั้งนี้มันก็ไม่ได้ง่าย ลองคิดเล่น ๆ ดูว่า ทุกคนต่างมีแผลใจในวัยเด็กกันทั้งนั้น บางคนใช้เวลารักษาแผลใจทั้งชีวิตยังรักษาไม่หาย ยังจำมันได้ขึ้นใจเจ็บปวดกับมัน ทรมานกับมัน ทำให้ไม่มีใครชอบแผลใจเหล่านี้ และการบูลลี่ คือ การที่สร้างแผลใจที่รักษาได้ยากนี้ให้กับคนอื่น

## สิ่งที่ทำให้เกิด การกลั่นแกล้งทางไซเบอร์ ได้จำนวนมาก คือ

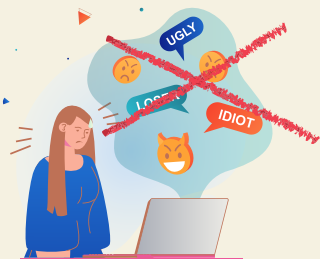
ความยากในการติดตาม และระบุตัวการ มันเป็นความสับสนอย่างหนึ่งที่เห็นผู้ถูกกระทำกระวนกระวายกับสิ่งที่เกิดขึ้น แต่หาต้นตอไม่เจอเนื่องจากคนทำสามารถซ่อนตัวตนบนโลกออนไลน์ได้และเมื่อมันเป็นกระแสก็จับมือใคร

ดมไม่ได้ ซึ่งมันง่ายมากที่จะโพสต์พุดถึงคนอื่น ยิ่งเป็นคนที่เราไม่ชอบหน้า เราก็รู้สึกว่าจะต้องถนอมน้ำใจ ยิ่งการแะการด่าอันนั้นมีจังหวะที่สนุก สะใจ หน่อย ๆ ทำให้วงสนทนามีความสุขสนาน มันก็รู้สึกว่าเป็นเรื่องที่ทำได้ และอาจเลยเถิดไปจนถึงการใส่สีตีไข่ ใส่ความเป็นคนไม่ดีให้ ชักจูงให้ทุกคนเกลียดคน ๆ นั้น จนนำไปสู่การลงมือกลั่นแกล้งในที่สุด

## ที่น่ากังวลคือ การบูลลี่ กันมืออยู่ แทบทุกสังคม ไม่เว้นแม้กระทั่งในสังคม ที่ทำงาน

- แพร่กระจายข่าวลือผิดเกี่ยวกับตัวเราในที่ทำงาน
- ดิสเครดิตเพื่อไม่ให้ได้รับความไว้วางใจ
- โปสต์ความเห็นเชิงลบเกี่ยวกับเรา จนเราเดือดร้อน
- ไม่ถูกยอมรับในที่ทำงาน ทุกคนตั้งแง่ และทิ้งให้โดดเดี่ยว
- หนักหน่อยหลายคนอาจจะเจอคอมเมนต์เชิงล้อเลียน หรือ Sexual Harassment จากคนในที่ทำงาน





## การจัดการกับ Cyberbully

ต้องเริ่มจาก **ความเข้าใจ** ว่า มันไม่ใช่เพียงการกลั่นแกล้งกันเล็กน้อยและไม่มีใครอยากให้เกิดกับตัวเอง เพราะร่องรอยดิจิทัลนี้สามารถอยู่ได้ตลอดไป มันไม่ได้หายไป มันลบไม่ได้ วันดีคืนดีก็จะย้อนกลับมา ยิ่งมันกลับมา ในช่วงที่เขื่อนึกว่าทุกอย่างมันดีขึ้นแล้ว ก็จะมีเจ็บปวดมากขึ้น

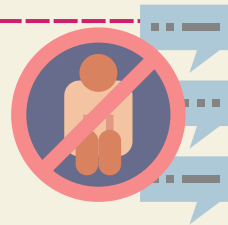
มีหลากหลายวิธีการ โดยอาศัยความร่วมมือระหว่างหน่วยงาน องค์กร ไม่แสวงหาผลกำไร โรงเรียน และชุมชนออนไลน์ เพื่อสร้างสภาพแวดล้อมที่ปลอดภัยและรับมือกับปัญหาการกลั่นแกล้งทางอินเทอร์เน็ต

ในต่างประเทศนั้น หลายประเทศได้พัฒนากฎหมาย และนโยบาย เพื่อต่อสู้กับ Cyberbully โดยเฉพาะ รวมถึงการกำหนดความผิดทางอาญาสำหรับการกลั่นแกล้งทางอินเทอร์เน็ต และการสร้างกรอบในการทำงานสำหรับโรงเรียน และองค์กรในการรายงานและจัดการกับเหตุการณ์ รวมไปถึง การรณรงค์วิธีการป้องกัน

รวมถึงการจัดการกับปัญหานี้ เป็นกลยุทธ์หลักที่สถานศึกษา และองค์กรต่าง ๆ มักจัดการรณรงค์เพื่อเพิ่มความตระหนักและสร้างทักษะการจัดการ

กับการกลั่นแกล้งในโลกไซเบอร์ พร้อมกันนี้ หลายแพลตฟอร์มออนไลน์และโซเชียลมีเดียได้พัฒนาเครื่องมือ ให้ผู้ใช้สามารถรายงานเนื้อหาที่เป็นการกลั่นแกล้งได้ง่ายขึ้น ทำให้ผู้ดูแลระบบสามารถดำเนินการลบเนื้อหาหรือบัญชีที่มีพฤติกรรมกลั่นแกล้งได้อย่างรวดเร็ว แต่สิ่งสำคัญ คือ การพัฒนาทักษะดิจิทัลและอารมณ์ให้กับเด็กและวัยรุ่น เพื่อช่วยให้พวกเขาสามารถจัดการกับสภาพแวดล้อมออนไลน์ได้อย่างปลอดภัยและเหมาะสม

## ตัวอย่างการจัดการปัญหา CYBERBULLY ในต่างประเทศ



### สหรัฐอเมริกา

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

## ออสเตรเลีย

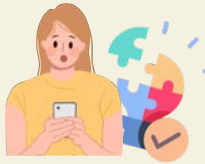
- มี eSafety Commissioner ซึ่งเป็นหน่วยงานของรัฐบาลที่รับผิดชอบในการป้องกันและต่อต้านการกลั่นแกล้งทางอินเทอร์เน็ต หน่วยงานนี้ให้บริการแนะนำ การสนับสนุน และทรัพยากรสำหรับผู้ที่ได้รับผลกระทบจาก Cyberbullying และมีอำนาจในการดำเนินการกับเนื้อหาที่เป็นการกลั่นแกล้งบนแพลตฟอร์มออนไลน์

## 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



# วิธีการรับมือ กับการกลั่นแกล้งทางไซเบอร์

**Stop**



คือหยุด ไม่ต้องไปตอบโต้ เสียเวลาไปใส่ใจกับคนนิสัยไม่ดีที่กลั่นแกล้งเรา หรือคุกคามเราทางออนไลน์ รวมทั้งบล็อกคนพวกนี้ไปเลยยิ่งดี

**Tell**



คือบอกหรือปรึกษาผู้ใหญ่ที่เราไว้วางใจหรือพูดคุยได้ ไม่ว่าจะพ่อแม่ ผู้ปกครอง หรือคุณครู

**Del ย่อมาจาก Delete**



คือบอกคนที่แกล้งให้ลบ ถ้าเขาไม่ลบก็แจ้งคุณครู หรือแจ้งให้ผู้ดูแลระบบ ลบโพสต์นั้นออก ที่สำคัญคือลบเรื่องที่ไม่เป็นจริงหรือทำร้ายจิตใจออกไป จากความคิดเราด้วย

**Strong**



คือยิ้มรับสิ่งที่เกิดอย่างเข้มแข็ง และใช้เป็นแรงผลักดันให้ชีวิตเราดีขึ้น

## สำหรับผู้ใหญ่ ผู้ปกครอง ครู อาจารย์ รวมทั้งคนแวดล้อม "Digital Resilience" หรือ ภูมิคุ้มกันในโลกดิจิทัล

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

### 1 ทักษะทางดิจิทัล (The Youth Digital Skill)

ความสามารถในการใช้เทคโนโลยีและการสื่อสารเพื่อผลิตผลงาน รวมถึง การเสพสื่อต่าง ๆ อย่างมีวิจารณญาณ

### 2 การมีภูมิคุ้มกันทางใจ (Resilience)

คือ ความสามารถในการรับมือและยืนหยัดเผชิญหน้ากับปัญหา จนสามารถ ฟื้นฟูจิตใจของตัวเองได้หลังจากผ่านเหตุการณ์เหล่านั้นไป

### 3 ปัจจัยปกป้องในการใช้สื่อดิจิทัล (Digital Protective Factor)

คือ สิ่งที่ช่วยทำให้เกิดการปรับตัวเพื่อสร้างเกราะป้องกันผลกระทบทางลบ

## หลักปฏิบัติ ที่ช่วยให้เราสามารถ จัดการกับความเสียหาย ที่อาจจะต้อง พบเจอได้ในอนาคต

มีด้วยกัน 4 ข้อ ดังนี้

1. รู้ตัวว่าเมื่อใดที่ตนเองตกอยู่ในความเสี่ยง
2. รู้ว่าต้องทำอะไรเพื่อขอความช่วยเหลือหากเจอภัยออนไลน์
3. เรียนรู้จากประสบการณ์ของตนเอง
4. รู้จักวิธีการกอบกู้สถานการณ์เมื่อเกิดปัญหา

ทั้งนี้ คนรอบตัวต้องเข้าใจถึงความร้ายแรงของเหตุการณ์ สิ่งที่สำคัญที่สุดไม่ใช่การดูดำ ไม่ว่าจะด้วยความโกรธหรือความเป็นห่วง แต่เป็นการรักษาจิตใจของคนที่เกี่ยวข้องทำให้สามารถรับมือปัญหาให้ผ่านพ้นไปได้

การไม่เป็นส่วนหนึ่งของการบูลลี่อาศัยแค่ตัวเราเท่านั้น แค่คิดว่า เรื่องนี้แชร์ออกไปแล้วจะทำร้ายใครไหม หลังจากนั้นก็มีคนที่นั่งอยู่เหมือนกัน คนที่อาจจะทั้งถูกหรือผิดก็ได้ ทุกอย่างอาจเป็นเรื่องเข้าใจผิดก็ได้ แต่คุณหยุดมือ และฉุกคิดก็ถือว่าเริ่มต้นที่ดีแล้ว





ปัญหาใหญ่ละเมิดสิทธิดิจิทัล  
 การแก่งกันข่มเหงทางไซเบอร์  
 ทั้งรูปแบบติดตามยามเมื่อเปลอ  
 พุดเพื่อเจ้าใส่ร้ายปลอมตัวตน  
 ทั้งคว่ำบาตรโต้เถียงเผยแพร่รูป  
 ส่งต่อรูปความรุนแรงเป็นวังวน  
 ผู้กระทำควรหยุดยั้งคิดกลับตน  
 ถ้าเป็นคนโดนบ้างจะเป็นไฉน ?!

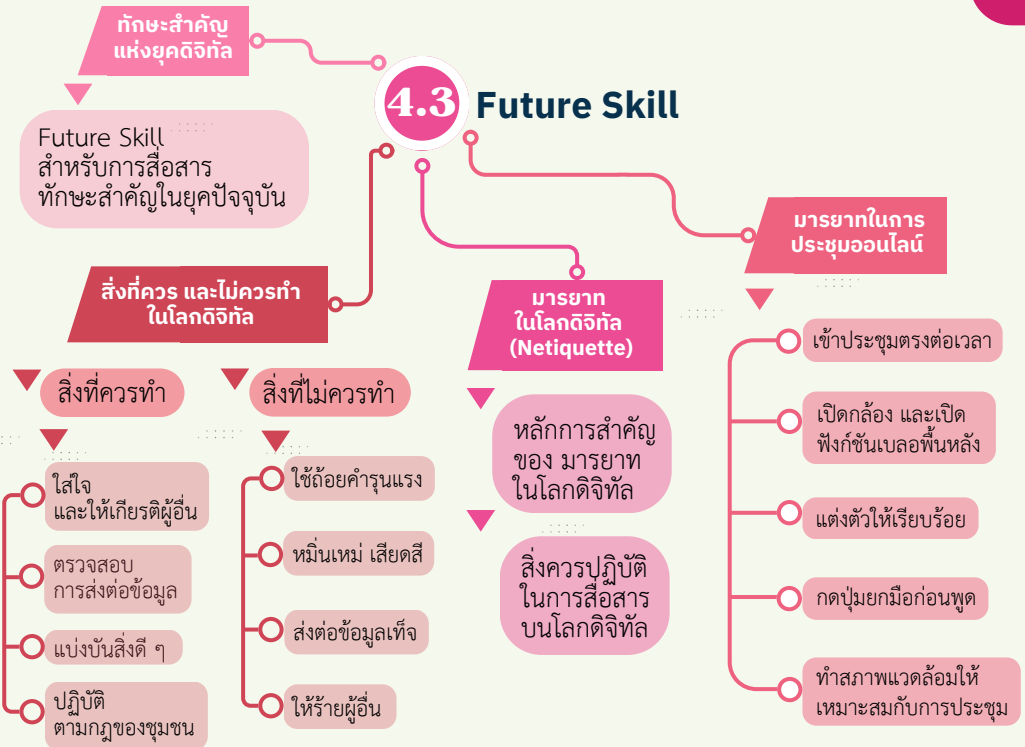
### 4.1 Digital Footprint Management



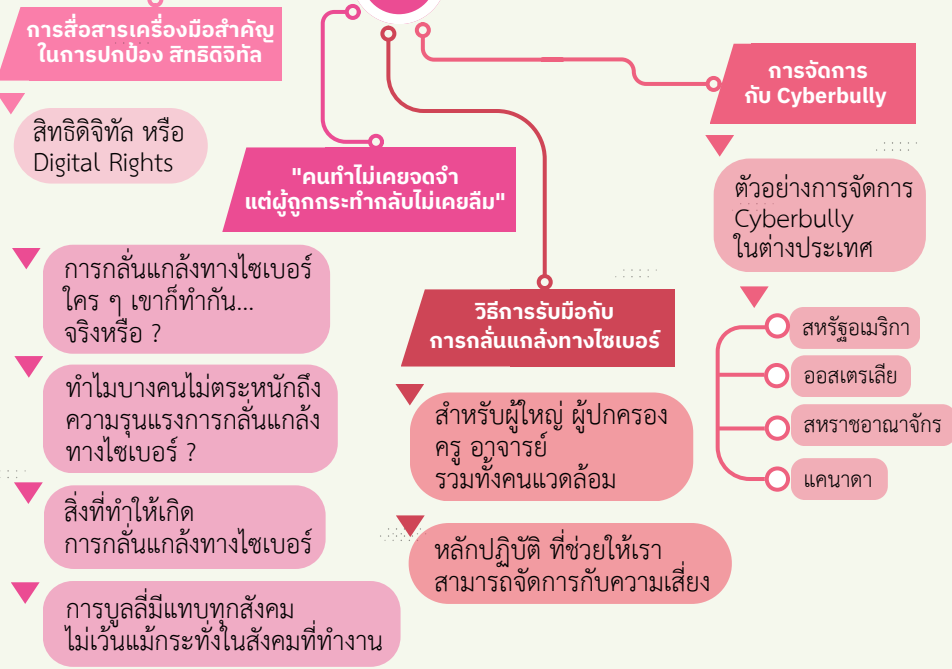
### 4.2 Interaction & Collaboration



### 4.3 Future Skill

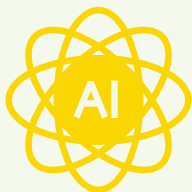
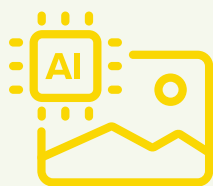
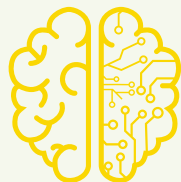


### 4.4 Cyberbully





05



# การรู้เท่าทันดิจิทัล

## Digital Literacy

# แนะนำสำหรับผู้สอน



## • วัตถุประสงค์

ผู้เรียนมีความรู้เกี่ยวกับผลกระทบที่เกิดขึ้น จากการนำเสนอเนื้อหาที่ไม่น่าเชื่อถือ และอธิบายถึงความแตกต่าง ความหลากหลายของแหล่งข้อมูล และความน่าเชื่อถือของข้อมูลที่รวบรวมจากสื่อดิจิทัลได้

## • ขอบเขตของเนื้อหาเรื่องนี้

### 5.1 Media & Information

- แหล่งข้อมูลดิจิทัล
- ธรรมชาติของสื่อ
- แนวทางในการรับชมสื่ออย่างรู้เท่าทัน
- การประเมินคุณภาพ / ความน่าเชื่อถือของข้อมูลจากสื่อดิจิทัล
- รู้เท่าทัน Fake News ป้องกันความเสี่ยงจากสื่อดิจิทัล
- แนวทางและแลกเปลี่ยนประสบการณ์ในการจัดการข้อมูลจากสื่อดิจิทัล
- การแบ่งปันเนื้อหาที่ไม่เหมาะสม

## 5.2 Digital Content Creation

- สื่อดิจิทัล
- แนวทางการสร้างเนื้อหาดิจิทัลให้ดีและโดนใจ
- แนวทางสร้างเนื้อหาดิจิทัลให้ดึงดูดและสร้างการจดจำ
- หลักการสร้างเนื้อหาให้ถูกกฎหมายและมีจริยธรรม
- พฤติกรรมการสร้างเนื้อหาและสื่อที่ละเมิดกฎหมาย
- ลิขสิทธิ์กับ CREATIVE COMMONS
- การอ้างอิงแหล่งข้อมูล (Citation) ในงานวิจัย

## 5.3 Data & AI Governance

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

เวลาในการเรียน

# รู้ศัพท์

## ไม่สับสน



1



### FAKE NEWS

คือ ข่าวปลอมหรือข่าวสารที่ไม่มีความจริง

2



### INFORMATION DISORDER

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

3



### MISINFORMATION

ข้อมูลที่ผิด คือ ข้อมูลที่ไม่ถูกต้อง หรือข้อมูลเท็จ โดยผู้ส่งอาจไม่รู้หรือไม่ได้ เจตนาต้องการเผยแพร่ข้อมูลที่ผิด

4



### DISINFORMATION

หรือข้อมูลที่ถูกบิดเบือน

คือ ข้อมูลที่ผู้ส่งตั้งใจสื่อสารออกมา อาจเป็นข้อมูลจริงบางส่วนที่เรียกว่า "ความจริงครึ่งเดียว" (HALF-TRUTH)

# รู้ศัพท์

## ไม่ลับสน



5



### MALINFORMATION

ข้อมูลที่แฝงเจตนาร้าย คือ ข้อมูลที่นำมาจากข้อเท็จจริง เพื่อนำมาทำร้ายเป้าหมาย โดยการนำข้อมูลความลับที่ละเมิดความเป็นส่วนตัวของผู้อื่นออกมาเปิดเผยในที่สาธารณะ เพื่อหวังที่จะโจมตีให้เกิดความเสียหายอับอาย

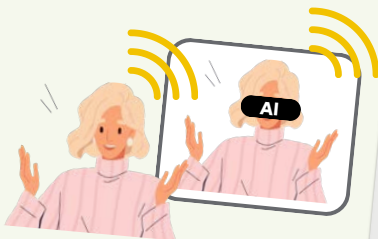
6



### DEEPPFAKE

คือ GENERATIVE AI รูปแบบหนึ่งที่สามารถสร้างสื่อสังเคราะห์ ทั้งภาพนิ่ง เสียง ภาพเคลื่อนไหวพร้อมเสียงที่เหมือนเป็นคนมาพูดหรือคุยจริง ๆ จนแทบแยกไม่ออก ด้วยระบบการเรียนรู้ หรือ DEEP LEARNING

7



### VOICE CLONING

คือ การใช้ AI ปลอมเสียง โดยจะเป็นการใช้ AI เลียนแบบเสียงของคุณคน ให้มีความคล้ายคลึงกับบุคคลจริง

8



### FAKE BUSINESS

คือ การใช้ GENERATIVE AI ในการสร้างบทความหรือสคริปต์วิดีโอ เพื่อให้ดูเหมือนมืออาชีพ



ถ้าคุณเรียนผ่านด้านนี้  
คุณจะมีภูมิคุ้มกัน  
ด้านข่าวลวงข้อมูลเท็จ  
และไม่ตกเป็นเหยื่อโจรออนไลน์

## 5.1

# MEDIA & INFORMATION

## วัตถุประสงค์

1. ผู้เรียนสามารถอธิบายถึงความแตกต่าง และหลากหลายของแหล่งข้อมูล และการได้มาซึ่งข้อมูลที่ตรงกับความต้องการบนโลกดิจิทัลได้
2. ผู้เรียนสามารถเข้าใจถึงวิธีการค้นหาข้อมูล รวบรวม และจัดการข้อมูล ที่ต้องการจากสื่อดิจิทัลได้
3. ผู้เรียนสามารถเข้าใจถึงการประเมินคุณภาพ และความน่าเชื่อถือของ ข้อมูล และเลือกใช้ข้อมูลที่สอดคล้องกับความต้องการได้
4. ผู้เรียนสามารถตระหนักถึงผลกระทบที่เกิดขึ้นจากการนำเสนอ หรือ แบ่งปันเนื้อหาที่ไม่น่าเชื่อถืออาจก่อให้เกิดความเข้าใจผิด หรือหลงเชื่อได้

# รู้เท่าทันดิจิทัล

SKILL

ทักษะจำเป็น

## เพื่อชีวิตออนไลน์



ในปัจจุบัน ที่เนื้อหาข้อมูลข่าวสารเพิ่มขึ้น และไหลผ่านอย่างรวดเร็ว อันเกิดจากสื่อที่มีมากขึ้น รวมถึง สื่อออนไลน์ที่ง่ายต่อการบริโภค และการส่งต่อ ดังนั้น “ความรู้เท่าทันดิจิทัล” จึงเป็นทักษะที่จำเป็นในการเข้าถึงแหล่งข้อมูลดิจิทัลให้ตรงกับความต้องการ เข้าใจ ประเมินค่า และใช้สื่อเหล่านี้อย่างมีประสิทธิภาพและปลอดภัย





# 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 เฟซบุ๊ก พันทิป หรือโซเชียลมีเดียต่าง ๆ เป็นต้น



### 2 แบ่งตามสิทธิการเข้าถึงข้อมูล

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

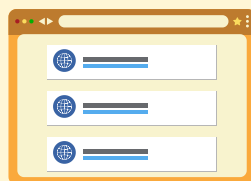
- แหล่งข้อมูลแบบคงที่ (Static)

คือ แหล่งข้อมูลที่มีรูปแบบการนำเสนอที่ตายตัว ไม่สามารถเปลี่ยนแปลงได้ เช่น เอกสาร PDF รูปภาพ วิดีโอ เป็นต้น



- แหล่งข้อมูลแบบไดนามิก (Dynamic)

คือ แหล่งข้อมูลที่มีรูปแบบการนำเสนอที่สามารถเปลี่ยนแปลงได้ เช่น เว็บไซต์ แอปพลิเคชัน เป็นต้น



## 5 แบ่งตามลักษณะการใช้งานได้

สามารถแบ่งได้ 2 ประเภท ได้แก่

- **แหล่งข้อมูลสาธารณะ (Public)**

คือ แหล่งข้อมูลที่สามารถเข้าถึงได้โดยไม่จำกัด เช่น เว็บไซต์ของรัฐบาล เว็บไซต์ขององค์กรต่าง ๆ เว็บไซต์ของสถาบันการศึกษา เป็นต้น



- **แหล่งข้อมูลส่วนตัว (Private)**

คือ แหล่งข้อมูลที่สามารถเข้าถึงได้เฉพาะผู้ที่มีสิทธิ์เท่านั้น เช่น เว็บไซต์ขององค์กรที่มีระบบรักษาความปลอดภัย 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 หรืออาจจะใช้คำที่หลากหลายขึ้นหากหาคำเดียวแล้วไม่พบ

### 3) เลือกใช้เครื่องมือค้นหาอย่างมีประสิทธิภาพและเจาะจง



เช่น ใช้ Google ค้นหาแบบทั่วไปหรือผ่านรูปภาพ และใช้ YouTube ค้นหา VDO

### 4) ใช้เครื่องมือค้นหาแบบขั้นสูง



เช่น ค้นหาข้อมูลตามช่วงเวลา ค้นหาข้อมูลตามภาษา

### 5) พิจารณาความน่าเชื่อถือและตรวจสอบความถูกต้องของข้อมูลก่อนนำไปใช้



โดยพิจารณาจากแหล่งที่มาของข้อมูล เนื้อหาของข้อมูล รูปแบบการนำเสนอข้อมูล เป็นต้น

### 6) ติดตามข่าวสารจากแหล่งข้อมูลที่น่าเชื่อถือ

ติดตาม

ทันสมัยและทันเหตุการณ์





# ธรรมชาติของสื่อ

สื่อเป็นเครื่องมือสำคัญในการถ่ายทอดข่าวสาร ข้อมูล และความรู้ไปยังผู้รับสาร สื่อมีบทบาทสำคัญต่อสังคม ทั้งในด้านการรับรู้ข่าวสาร เสริมสร้างความรู้ความเข้าใจ และการสร้างค่านิยมความเข้าใจธรรมชาติของสื่อ จึงเป็นสิ่งสำคัญสำหรับผู้คนในยุคปัจจุบัน

## ประเภทของธรรมชาติของสื่อ

สามารถแบ่งออกเป็น 5 ประเภท

### 1 สื่อ คือ สิ่งที่ถูกสร้างขึ้นมาจากมนุษย์

อาศัยความเชื่อและทัศนคติของผู้สร้าง จึงสามารถมีความลำเอียง หรืออคติได้ เช่น โฆษณาหรือสินค้าที่เกินจริง การนำเสนอข่าว ที่เอื้อต่อกลุ่มผู้มีอำนาจ เป็นต้น





## 2 สื่อส่วนใหญ่ที่มีเป้าหมายธุรกิจ

จะมีวัตถุประสงค์เพื่อหารายได้ เน้นดึงดูดความสนใจผู้คน การที่สื่อมีเป้าหมายแบบนี้ เราต้องตระหนักว่า มันเป็นสื่อเพื่อความบันเทิง อาจจะวัดเรื่องความถูกต้องหรือเป็นกลางไม่ได้ เช่น โฆษณา รายการเกมโชว์

## 3 สื่อสร้างค่านิยมและอุดมคติ

ตระหนักไว้เสมอว่าสื่ออาจส่งผลต่อความคิดและพฤติกรรมของเรา เช่น Soft Power ที่เกิดจากอุตสาหกรรมความบันเทิง (ภาพยนตร์ ละครโทรทัศน์ เพลง) เป็นต้น



## 4 สื่อทำให้เกิดผลทางการเมืองและสังคม

สื่อจึงอาจถูกใช้เป็นเครื่องมือในการโฆษณาชวนเชื่อหรือสร้างความแตกแยกในสังคม เราจึงควรใช้วิจารณญาณในการรับชมสื่อ เช่น ในช่วงเลือกตั้ง สื่อบางสื่ออาจถูกใช้เป็นเครื่องมือในการปลุกปั่นแพร่กระจายข้อมูลที่เข้าข้างพรรคการเมือง หรือข้อมูลที่เบี่ยงเบน เพื่อหวังผลทางการเมือง



## 5 สื่อมีเอกลักษณ์และข้อจำกัดเฉพาะตัว

สื่อบางประเภทอาจนำเสนอข้อมูลได้ละเอียดและรอบด้าน บางประเภทอาจจะเน้นความรวดเร็วเป็นหลัก การเข้าใจเอกลักษณ์นี้ จะทำให้เราเลือกรับสื่อได้อย่างเหมาะสม เช่น



- สื่อประเภทสิ่งพิมพ์ จะใช้เทคนิคทางคอมพิวเตอร์เพื่อปรับแต่งภาพใหม่ให้ลงตัว หรือใช้คำที่สร้างอารมณ์ความรู้สึก
- สื่อประเภทภาพยนตร์ ละครทีวี หนังสือ จะใช้การตัดต่อภาพ เสียง แสงไฟ มุมกล้อง 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

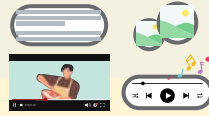
#### 1 แหล่งที่มาของข้อมูล

มีการระบุชื่อและที่อยู่ของแหล่งที่มาอย่างชัดเจน สามารถตรวจสอบได้ มีประวัติการเผยแพร่ข้อมูลที่เป็นจริง

#### 2 เนื้อหาของข้อมูล

ควรเป็นเนื้อหาที่มีความถูกต้อง ครบถ้วน มีแหล่งอ้างอิง นำเสนออย่างเป็นกลาง ไม่มีลักษณะอคติหรือชี้นำ ใช้ภาษาถูกต้องเหมาะสม

### 3 รูปแบบการนำเสนอข้อมูล



ต้องมีความเข้าใจง่าย ไม่ซับซ้อน มีการจัดระเบียบข้อมูล  
อย่างเป็นระบบ

### 4 ปฏิกริยาของผู้คน



หากข้อมูลได้รับความสนใจจากคนจำนวนมาก ในเชิงบวก  
แสดงว่าข้อมูลนั้นมีความน่าเชื่อถือมากขึ้น

### 5 ความถี่ของการเผยแพร่ข้อมูล



หากข้อมูลมีการเผยแพร่ซ้ำ ๆ จากแหล่งที่มาที่แตกต่างกัน  
แสดงว่าข้อมูลนั้นมีความน่าเชื่อถือมากขึ้น

# รู้เท่าทัน Fake News ป้องกันความเสี่ยงจากสื่อดิจิทัล



## Fake News คืออะไร ?

### REMEMBER

คำว่า Fake News ไม่ได้หมายถึงข่าวที่ไม่จริงเท่านั้น แต่ยังรวมถึง ข้อมูลต่าง ๆ ที่ไม่เป็นความจริงด้วย

## Claire Wardle จาก First Draft

ซึ่งเป็นองค์กรทำงานต่อต้านข่าวลวงและข้อมูลเท็จเพื่อสร้างความไว้วางใจและความจริงในยุคดิจิทัล ระบุว่า การที่จะเข้าใจระบบนิเวศของการส่งต่อหรือแชร์ข้อมูลข่าวสารผิด ๆ ออกไปนั้น ควรจะ **ต้องทำความเข้าใจกับประเภทของข่าวสารข้อมูลเท็จ แรงจูงใจของคนทำและการแพร่กระจายของเนื้อหา**



## ลักษณะของ Fake News

1



มีเนื้อหาที่เกินจริง  
หรือบิดเบือนความจริง

2



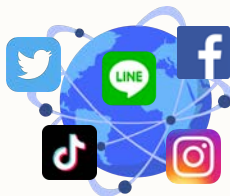
สร้างความตื่นตระหนก  
หรือสร้างความแตกแยก

3



เล่นกับความสงสัย

4



มีการเผยแพร่ผ่าน  
สื่อสังคมออนไลน์เป็นหลัก

## ข้อมูลเท็จมาจากไหน ?

มาจากหลากหลายแง่มุม เช่น

- แง่มุมเจตนา : จงใจให้ข้อมูลเท็จ หรือให้ข้อมูลเท็จโดยรู้เท่าไม่ถึงการณ์
- แง่มุมเหตุผลเบื้องหลัง : ทำเพื่อเงิน เพื่อชู้หน้า เพื่อความสุข หรือเพราะความหวังดีที่ขาดความรู้

- แง่มุมความถูกต้อง : คาดเคลื่อนทั้งหมด หรือคาดเคลื่อนบางส่วน
- แง่มุมกรอบเวลา : ข้อมูลเก่า ข้อมูลใหม่ ข้อมูลที่เป็นจริงในอดีต
- แง่มุมแหล่งกำเนิด : ปากต่อปาก ไลน์ เฟซบุ๊ก โซเชียลมีเดียต่าง ๆ

องค์การอนามัยโลก ได้บัญญัติศัพท์ออกมาใช้สื่อถึงการระบาดของข้อมูลข่าวสารที่ไม่ถูกต้อง คลาดเคลื่อนหรือบิดเบือนเกี่ยวกับโรคติดเชื้อไวรัสโคโรนา คือคำว่า การแพร่ระบาดของข่าวสาร หรือ “Infodemic” เป็นการรวมคำสองคำเข้าด้วยกันจาก Information (ข่าวสาร) และคำว่า Epidemic (การระบาด) โดยข้อมูลในลักษณะนี้ถือเป็นความผิดปกติของข้อมูลข่าวสาร (Information Disorder)

นอกจากนี้สหภาพยุโรปยังได้ขยายความ Information Disorder ออกเป็น 3 ประเภท ได้แก่

1 **Misinformation** หรือข้อมูลที่ผิด



2 **Disinformation** หรือข้อมูลบิดเบือน



3 **Malinformation** หรือข้อมูลที่แฝงเจตนาร้าย



## ประเภทของข้อมูลเท็จ

### 1 ข่าวปลอม (Fabricated Content)

กุเรื่องมั่วทั้งหมด มุ่งหลอกลวง



### 2 ชี้นำ (Misleading Content)

จัดฉากข้อมูลเพื่อชี้นำ ใส่ร้าย



### 3 โยงมั่ว (False Connection)

ไม่สัมพันธ์กันระหว่างพาดหัว ภาพ คลิป หรือคำบรรยายประกอบ



### 4 ผิดบริบท (False Context)

เป็นข้อมูลจริง แต่นำมาใช้ผิดบริบท



### 5 ล้อเลียน (Satire & Parody)

เนื้อหาเสียดสีให้เกิดความตลกขบขัน ไม่มุ่งให้เกิดอันตราย แต่อาจทำให้บางคนหลงเชื่อว่าเป็นความจริง



### 6 สวมรอย (Imposter Content)

ปลอมตัวสวมรอยให้ข้อมูล เพื่อหลอกลวงหรือหวังร้าย



### 7 หลอกลวง (Manipulated Content)

สร้างแต่งตัดข้อมูล เพื่อหลอกลวงโดยเฉพาะ



## สาเหตุที่มาของข้อมูลเท็จ



1. การขาดทักษะความรู้เท่าทัน การเผยแพร่ และวิเคราะห์ข่าวหรือสารสนเทศอื่น ๆ
2. ต้องการปลุกปั่นยุยง
3. ข้อมูลเลือกข้าง
4. เพื่อชี้นำทางการเมือง
5. ความต้องการเสียดสีเพื่อความขบขัน
6. เพื่อสนองความพึงพอใจ
7. เพื่อสร้างรายได้
8. เพื่อโฆษณาชวนเชื่อ

## การตรวจสอบเบื้องต้น

### 1 ตรวจสอบแหล่งที่มาของข่าวสารข้อมูล

เช่น สำนักข่าว หน่วยงาน ชื่อผู้ให้ข้อมูลมีความน่าเชื่อถือ เป็นต้น

### 2 ตรวจสอบแหล่งข้อมูลอื่น ๆ ประกอบ

เช่น หน่วยงานราชการหรือหน่วยงานที่น่าจะเกี่ยวข้องกับข่าวสารข้อมูลนั้น ๆ เพื่อยืนยันว่ามีเรื่องหรือเหตุการณ์ดังกล่าวจริง

### 3 ตรวจสอบหาต้นตอของข่าว

บางครั้งข่าวเท็จอาจเป็นข่าวเก่าที่เคยเกิดขึ้นแล้วหรือใช้ข้อมูลจากข่าวเก่ามาเล่าใหม่ เพื่อให้เกิดความแตกตื่นหรือเพื่อประโยชน์แอบแฝง

### 4 สอบถามผู้เชี่ยวชาญในเรื่องนั้น ๆ โดยตรง

หรือหาข้อมูลเพิ่มเติมจากแหล่งที่เชื่อถือได้

# สาเหตุที่มาของข้อมูลเท็จ

คำแนะนำในการรับมือกับข่าวปลอม

1. อย่าเชื่อข้อมูลที่เห็นหรือได้ยินในทันที



2. ตรวจสอบแหล่งที่มาของข้อมูล ก่อนจะกดแชร์หรือเผยแพร่



3. ใช้วิจารณญาณในการรับข้อมูล



4. หากพบเห็นข่าวปลอม ควรรายงานไปยังหน่วยงานที่เกี่ยวข้อง



ทั้งนี้บางครั้งคนก็เผยแพร่เนื้อหาออกไปโดยไม่รู้ว่าเป็น **Misinformation** ที่ข้อมูลผิดหรือถูกบิดเบือน เพียงเพราะความปรารถนาดีต่อสังคมดิจิทัล

# แนวทางในการรับชมสื่อ อย่างรู้เท่าทัน

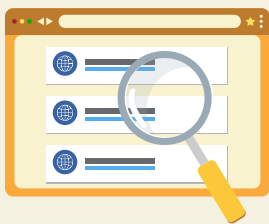
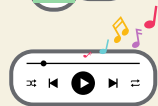


การเข้าใจธรรมชาติของสื่อ จะช่วยให้เราสามารถรับชมสื่อได้อย่างรู้เท่าทัน เราสามารถวิเคราะห์เนื้อหาของสื่อได้อย่างมีวิจารณญาณ และเราสามารถเลือกรับสื่อที่เป็นประโยชน์ต่อตนเองและสังคม

## แนวทางในการรับชมสื่ออย่างรู้เท่าทัน มีดังนี้

### 1 ตระหนักถึงธรรมชาติของสื่อ

ก่อนรับชมสื่อใด ๆ ควรตระหนักถึงธรรมชาติของสื่อ นั้น ๆ ว่า สื่อ นั้น ถูกสร้างขึ้นโดยใคร มีเป้าหมายอย่างไร และอาจส่งผลกระทบต่อตนเองและสังคม



### 2 ตรวจสอบแหล่งที่มาของข้อมูล

ก่อนเชื่อข้อมูลใด ๆ ที่ได้รับจากสื่อ ควรตรวจสอบแหล่งที่มาของข้อมูลว่าเชื่อถือได้หรือไม่

### 3 ใช้วิจารณญาณในการรับชมสื่อ

ไม่ควรเชื่อข้อมูลของสื่ออย่างทันที ควรใช้ วิจารณญาณในการตีความข้อมูลและพิจารณา ว่าข้อมูลนั้นสอดคล้องกับความเป็นจริงหรือไม่

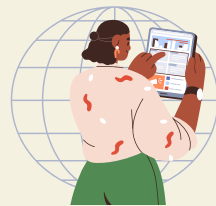


### 4 ไม่ควรรับชมสื่อจากแหล่งเดียว

ควรรับชมสื่อจากแหล่งต่าง ๆ ที่หลากหลาย เพื่อให้ได้มุมมองที่หลากหลาย

### 5 มีส่วนร่วมในการแลกเปลี่ยนข้อมูล

เราสามารถมีส่วนร่วม ในการแลกเปลี่ยนข้อมูล กับผู้อื่น เพื่อแลกเปลี่ยนมุมมองและความคิดเห็น เกี่ยวกับสื่อต่าง ๆ





# ศิลปะแห่งการจัดการ ข้อมูลจากสื่อดิจิทัล ด้วยตนเอง

การให้ความสำคัญกับข้อมูลส่วนบุคคล ข้อมูลการทำงาน และข้อมูลที่เกี่ยวข้องกับความสำเร็จของกิจกรรมต่าง ๆ เป็นบทบาทที่สำคัญในการบริหารชีวิตที่มีประสิทธิภาพ

## มาสำรวจแนวทาง และแลกเปลี่ยนประสบการณ์ใน การจัดการข้อมูล ด้วยตนเองกัน !

### 1 กำหนดและบริหารข้อมูลส่วนบุคคล

ก่อนรับชมสื่อใด ๆ ควรตระหนักถึงธรรมชาติของสื่อ นั้น ๆ ว่า สื่อ นั้น ถูกสร้างขึ้นโดยใคร มีเป้าหมายอย่างไร และอาจส่งผลกระทบต่อตนเอง และสังคม

### 2 ใช้เทคโนโลยีเพื่อจัดการข้อมูล

โดยใช้แอปพลิเคชันหรือเทคโนโลยีต่าง ๆ ช่วย

### 3 การจัดหมวดหมู่ และสร้างระบบข้อมูล

ใช้ชื่อไฟล์และโฟลเดอร์ที่ชัดเจน และการสร้างระบบที่เข้าใจง่ายช่วยให้ ค้นหาข้อมูลเป็นเรื่องง่าย

#### 4 การสำรวจและลบข้อมูลที่ไม่จำเป็น

ทุก ๆ ครั้งที่ได้รับข้อมูลเพิ่มมากขึ้น ควรทำการตรวจสอบ และลบข้อมูลที่ไม่จำเป็นออก

#### 5 การสร้างนิสัยการสำรวจและปรับปรุง

เราสามารถมีส่วนร่วมในการแลกเปลี่ยนข้อมูลกับผู้อื่น เพื่อแลกเปลี่ยนมุมมองและความคิดเห็นเกี่ยวกับสื่อต่าง ๆ

#### 6 การทำสำเนาข้อมูล (Backup)

การทำสำเนาข้อมูลเป็นการป้องกันการสูญหายข้อมูลที่สำคัญ 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 หรือจารีตประเพณี ของสังคม เช่น เนื้อหาลามกอนาจาร เนื้อหาที่สร้างความแตกแยกหรือเกลียดชัง เนื้อหาที่เผยแพร่ข้อมูลเท็จหรือบิดเบือนความจริง เป็นต้น

### ผลกระทบการแบ่งปันเนื้อหาที่ไม่เหมาะสม

01

#### สร้างความเสียหายต่อบุคคลอื่น



เนื้อหาที่ไม่เหมาะสมบางประเภทอาจสร้างความเสียหายต่อบุคคลอื่น เช่น เนื้อหาลามกอนาจาร อาจทำให้บุคคลอื่นรู้สึกอับอายหรือถูกละเมิด เนื้อหาที่สร้างความแตกแยก หรือเกลียดชังอาจทำให้บุคคลอื่นรู้สึกเกลียดชังหรือถูกรังแก เป็นต้น

EXAMPLE



## ตัวอย่างที่เห็นได้ชัด เช่น

- กรณีนำภาพของบุคคลไปเผยแพร่โดยไม่ได้รับอนุญาต หรือ การนำภาพหรือวิดีโอลามกอนาจารของบุคคล ไปเผยแพร่ ซึ่งอาจทำให้บุคคลนั้นรู้สึกอับอาย หรือถูกละเมิด ในกรณีที่รุนแรงอาจนำไปสู่การฆ่าตัวตายได้
- กรณีที่มีการเผยแพร่ข้อความ หรือเนื้อหาที่สร้างความแตกแยกหรือเกลียดชัง ซึ่งอาจทำให้บุคคลอื่น รู้สึกถูกเกลียดชัง หรือถูกรังแก

EXAMPLE

## จับแล้วหนุ่มหลอกเด็ก 17 ถ่ายคลิปโป๊แบล็กเมลรีดเงิน



หลอกถ่ายคลิปโป๊แบล็กเมล

รวบแล้วหนุ่มแสบหลอกนักเรียนชายวัย 17 ปี ถ่ายคลิปโป๊แล้วแบล็กเมลรีดเงินหลายครั้งจนเด็กคิดสั้น พบประวัติก่อเหตุโซเชียล มีผู้ตกเป็นเหยื่อเกือบ 20 ราย

## EXAMPLE

ผู้ต้องหารับสารภาพว่า ใช้วิธีปลอมโปรไฟล์ในอินสตาแกรม เป็นภาพหญิงสาวหน้าตาดีและไปหาเหยื่อในแชตลับหาคู่ จนพบกับเหยื่อเมื่อปลายเดือนมกราคมที่ผ่านมา จึงแชตตีสนิท พูดคุยหลอกล่อชักชวนขอมีเพศสัมพันธ์ แต่ขอให้เหยื่อถ่ายคลิปรูปร่างไปเปลือยมาให้ดูก่อน เมื่อเหยื่อหลงเชื่อ จึงข่มขูรีดไถเงิน ครั้งละ 4,000-5,000 บาท ไม่เช่นนั้นจะเผยแพร่ภาพคลิปในโซเชียลได้เงินไปกว่า 20,000 บาท จนเมื่อวันที่ 13 มีนาคมที่ผ่านมา ได้ข่มขู่เหยื่อขอเงินอีก 20,000 บาท จนเหยื่อเกิดความเครียดใช้อาวุธปืนของพ่อปลิดชีพตัวเอง

## 02

## สร้างความเสียหายต่อสังคมโดยรวม



เนื้อหาที่ไม่เหมาะสม อาจสร้างความเสียหายต่อสังคมโดยรวม เช่น เนื้อหาที่เผยแพร่ข้อมูลเท็จ หรือบิดเบือนความจริงอาจทำให้สังคมเกิดความสับสนและแตกแยก เนื้อหาที่ส่งเสริมความรุนแรง อาจทำให้สังคมเกิดความวุ่นวายและอาชญากรรม เป็นต้น

## EXAMPLE

## ตัวอย่างที่เห็นได้ชัด เช่น



กรณีที่มีการนำข่าวปลอมไปเผยแพร่ ซึ่งอาจทำให้ประชาชนเกิดความสับสนและแตกแยก เช่น

- การนำข่าวปลอมเรื่องการแพร่ระบาดของโรคระบาดไปเผยแพร่ ซึ่งอาจทำให้ประชาชนเกิดความตื่นตระหนก และกักตุนสินค้า
- การนำข่าวปลอมเรื่องการเลือกตั้งไปเผยแพร่ ซึ่งอาจทำให้ประชาชนเกิดความแตกแยกและนำไปสู่ความรุนแรงได้
- กรณีที่มีการนำภาพหรือวิดีโอความรุนแรง ไปเผยแพร่ ซึ่งอาจทำให้สังคมเกิดความหวาดกลัว และอาจนำไปสู่การส่งเสริมความรุนแรง เช่น การนำภาพหรือวิดีโอการฆ่าตัวตายไปเผยแพร่ ซึ่งอาจทำให้เยาวชนเกิดความคิดที่จะฆ่าตัวตายได้

## 03

## ส่งผลกระทบต่อผู้แบ่งปันเนื้อหา



ผู้แบ่งปันเนื้อหาที่ไม่เหมาะสม อาจถูกดำเนินคดีทางกฎหมายหรือถูกสั่งคุมประณาม เช่น หากแบ่งปันเนื้อหาลามกอนาจาร อาจถูกดำเนินคดีฐานผลิตหรือเผยแพร่สื่อลามกอนาจาร หากแบ่งปันเนื้อหาที่สร้างความแตกแยกหรือเกลียดชัง อาจถูกดำเนินคดีฐานยุยงปลุกปั่น หากแบ่งปันเนื้อหาที่เผยแพร่ข้อมูลเท็จหรือบิดเบือนความจริง อาจถูกดำเนินคดีฐานหมิ่นประมาท เป็นต้น

ดังนั้น จึงควรระมัดระวังในการแบ่งปันเนื้อหาบนอินเทอร์เน็ต ตรวจสอบให้แน่ใจว่าเนื้อหาที่แบ่งปันนั้นไม่เหมาะสมต่อผู้อื่นหรือสังคมโดยรวม หากพบเห็นเนื้อหาที่ไม่เหมาะสม ควรแจ้งให้หน่วยงานที่เกี่ยวข้องทราบ เพื่อดำเนินการจัดการอย่างเหมาะสม

**มาดูกันว่า** การใช้งานหรือ

เผยแพร่ข้อมูลใดบ้าง ที่ทำบนโลกดิจิทัล

แล้วขัดต่อกฎหมาย หรือขัดต่อจริยธรรม



<b>การกระทำ/พฤติกรรม</b> 	<b>ผลกระทบ ทางกฎหมาย</b> 	<b>ผลกระทบ ทางจริยธรรม</b> 
<p>ฝากร้าน ขายของ และส่งข้อความก่อกวน โดยไม่ได้รับอนุญาต หรือผู้รับปฏิเสธไม่ได้</p>	<p>มีความผิดปรับไม่เกิน 2 แสนบาท</p>	<p>ทำให้ผู้อื่น เกิดความรำคาญ</p>
<p>โพสต์ หรือแชร์ข้อมูลเท็จ ที่สร้างความเสียหาย ต่อบุคคล หรือประเทศ</p>	<p>จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสน และระงับข้อมูลนั้น</p>	<p>เกิดความเข้าใจผิด อับอาย สร้างความเกลียดชัง ทำให้เสื่อมเสียชื่อเสียง</p>
<p>โพสต์ข้อมูลปลอม ทูจจริต หลอกลวงสร้างความเสียหาย ด้านความมั่นคง</p>	<p>จำคุกไม่เกิน 5 ปี ปรับไม่เกิน 1 แสน และระงับข้อมูลนั้น หรือ บทลงโทษตามมาตรา ที่เกี่ยวข้อง</p>	<p>เกิดความตื่นตระหนก การขัดแย้งทางสังคม ทำให้การตัดสินใจ ผิดพลาดได้</p>
<p>โพสต์ หรือแชร์ข้อมูล ภาพตัดต่อ ที่สร้างความเสื่อมเสียต่อผู้อื่น รวมถึงผู้เสียชีวิต</p>	<p>จำคุกไม่เกิน 3 ปี หรือปรับไม่เกิน 2 แสน และระงับข้อมูลนั้น</p>	<p>สร้างความอึดอัดใจ ความสะเทือนใจ และความรู้สึกหดหู่ใจ</p>

<p><b>การกระทำ/พฤติกรรม</b></p> 	<p><b>ผลกระทบ ทางกฎหมาย</b></p> 	<p><b>ผลกระทบ ทางจริยธรรม</b></p> 
<p>โพสต์หรือแชร์ภาพไป เปลือย ลามกอนาจาร การพนัน</p>	<p>จำคุกไม่เกิน 5 ปี หรือปรับไม่เกิน 1 แสน หรือทั้งจำทั้งปรับ และระงับข้อมูลนั้น</p>	<p>ทำให้ผู้อื่นเกิดความวิตก กังวล อับอาย เสียชื่อเสียง</p>
<p>โพสต์ แชร์ หรือขาย โปรแกรม เพลง ภาพยนตร์ โดยไม่ได้รับอนุญาต</p>	<p>ความผิดด้านลิขสิทธิ์ จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 2 หมื่น หรือทั้งจำทั้งปรับ</p>	<p>ถือเป็นการขโมย ลิขทรัพย์ ทำให้ผู้อื่นเสียผลประโยชน์</p>
<p>การส่งข้อความทำธุรกรรม ทางการเงิน เช่น แชตยืมเงิน ถือเป็นหลักฐาน หรือสัญญาทางการเงิน</p>	<p>หากไม่คืนหรือทำตาม ข้อตกลง เจ้าหนี้ฟ้องร้อง ทางแพ่ง เพื่อเรียกเงินคืนได้ ตาม พ.ร.บ. ธุรกรรม ทางอิเล็กทรอนิกส์</p>	<p>ทำให้ผู้อื่นเกิดความ เดือดร้อน ไม่สบายใจ วิตกกังวล กลัวว่าจะเสียทรัพย์</p>
<p>การกด Like กด Share ถือเป็นการเผยแพร่ข้อมูล หากข้อมูลนั้นเป็นข้อมูล ปลอม เท็จ นั้นเท่ากับว่า เราผิดกฎหมาย พ.ร.บ. แล้ว</p>	<p>จำคุกไม่เกิน 5 ปี หรือ ปรับไม่เกิน 1 แสน หรือ ทั้งจำทั้งปรับ</p>	<p>ทำให้ผู้อื่นเกิดความ ไม่สบายใจ เสื่อมเสียชื่อเสียง</p>



รู้เท่าทันใช้ข้อมูลอย่างปลอดภัย  
 คลายสงสัยให้สืบค้นแหล่งศูนย์  
 ให้ใช้หลักการเข้าถึงช่วยเกื้อกูล  
 จะเพิ่มพูนความรู้จักทักษะพราว  
 กำหนดวัตถุประสงค์ใส่คำค้น  
 ใช้เครื่องมือมากลั่นสนใจข่าว  
 ต้องระวังข้อมูลเท็จแฮร์เรื่องราว  
 ควรสืบสาวก่อนใช้ดูให้ดี



ถ้าคุณเรียนผ่านด้านนี้  
คุณจะได้สร้างสื่อได้ปังและโดนใจ  
ไม่เสี่ยงทำผิดกฎหมายด้านลิขสิทธิ์  
ที่มีโทษสูงทั้งจำและปรับ

# 5.2

## DIGITAL CONTENT CREATION

### วัตถุประสงค์

1. ผู้เรียนสามารถอธิบายวิธีการสร้างเนื้อหา หรือสื่อดิจิทัลสอดคล้องกับวัตถุประสงค์ในการนำไปใช้และประเด็นกฎหมายที่เกี่ยวข้อง เช่น ลิขสิทธิ์ สัญญาอนุญาตแบบเปิด (CREATIVE COMMONS) ได้
2. ผู้เรียนสามารถเข้าใจถึงการผลิต หรือสร้างสรรค์เนื้อหาหรือสื่อดิจิทัลที่สอดคล้องกับวัตถุประสงค์ ให้เกิดประโยชน์ในการนำไปใช้และสังคมได้
3. ผู้เรียนสามารถตระหนักถึงจรรยาบรรณในการนำผลงาน 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)

วิดีโอคลิป ภาพยนตร์ รายการทีวี สตรีมมิง

## 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 วิดีโอคอล การประชุมทางไกล

### 4. ด้านธุรกิจ (Business Content)

เว็บไซต์ โฆษณาออนไลน์ อีเมลการตลาด บทความบล็อก

## รูปแบบการนำเสนอ ของสื่อและเนื้อหาดิจิทัล

สามารถเผยแพร่ผ่านช่องทางต่าง ๆ มากมาย ขึ้นอยู่กับกลุ่มเป้าหมายและวัตถุประสงค์ ตัวอย่างช่องทางการเผยแพร่ ได้แก่

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

## ตัวอย่างการใช้งานสื่อและเนื้อหาดิจิทัล

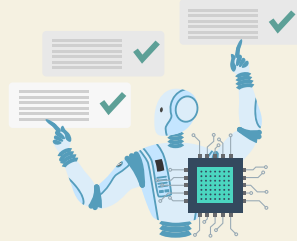
**การศึกษา :** สามารถเรียนออนไลน์ ผ่านเว็บไซต์ หรือแอปพลิเคชันต่าง ๆ และสามารถใช้อีสื่อดิจิทัลเพื่อประกอบการสอนได้ เช่น วิดีโอ อินโฟกราฟิก เกม เป็นต้น

**ความบันเทิง :** สามารถฟังเพลง ดูหนัง เล่นเกม ผ่านแพลตฟอร์มดิจิทัลต่าง ๆ

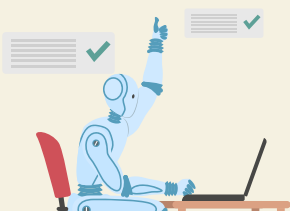
**การสื่อสาร :** สามารถติดต่อสื่อสารกันผ่านโซเชียลมีเดีย แอปพลิเคชัน ส่งข้อความ และโปรแกรมประชุมออนไลน์

**ธุรกิจ :** สามารถใช้อีสื่อดิจิทัลเพื่อการโฆษณา 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 ?

ในยุคดิจิทัลที่ข้อมูลข่าวสารไหลบ่า ผู้คนสามารถเข้าถึงสื่อและเนื้อหาต่าง ๆ ได้อย่างสะดวกรวดเร็ว สื่อจึงมีบทบาทสำคัญในการกำหนดทิศทาง ความคิด และพฤติกรรมของสังคม

## สื่อหรือเนื้อหา ที่เกิดประโยชน์กับสังคม

หมายถึง สื่อหรือเนื้อหาที่ส่งผลดีต่อสังคม ช่วยพัฒนาคุณภาพชีวิต และส่งเสริมความเจริญก้าวหน้าในด้านต่างๆ

### ลักษณะของสื่อหรือเนื้อหา ที่เกิดประโยชน์กับสังคม

#### 1 นำเสนอข้อมูลข่าวสารที่ถูกต้อง ครบถ้วนและเป็นกลาง



- ตรวจสอบข้อเท็จจริงก่อนนำเสนอ
- อ้างอิงแหล่งที่มาของข้อมูล
- นำเสนอเนื้อหาอย่างตรงไปตรงมา ไม่บิดเบือน
- นำเสนอหลายแง่มุมของประเด็น

#### 2 ส่งเสริมความรู้ ความคิดสร้างสรรค์ และทักษะชีวิต



- เนื้อหามีคุณค่า สาระประโยชน์
- กระตุ้นให้คิดวิเคราะห์
- พัฒนาทักษะการคิดสร้างสรรค์
- ส่งเสริมทักษะจำเป็นสำหรับชีวิต

3

### สร้างสรรค์สังคมแห่งการเรียนรู้



- กระตุ้นให้ใฝ่รู้ ใฝ่เรียน
- สนับสนุนการศึกษา
- แบ่งปันความรู้
- ส่งเสริมการอ่าน

4

### ยกย่องคุณธรรม จริยธรรม และค่านิยมที่ดีงาม



- เนื้อหาสอดคล้องกับค่านิยมที่ดีงาม
- ส่งเสริมความดีงาม
- ยกย่องบุคคลต้นแบบ
- กระตุ้นให้ทำความดี

5

### สร้างความสามัคคี ประองดอง และความเข้าใจในสังคม



- เนื้อหาส่งเสริมความหลากหลาย
- หลีกเลี่ยงการแบ่งแยก
- กระตุ้นการรับฟัง
- ส่งเสริมการอยู่ร่วมกันอย่างสันติ

6

## กระตุ้นให้มีส่วนร่วม ในการพัฒนาสังคม



- นำเสนอปัญหาในสังคม
- กระตุ้นให้คิดหาวิธีแก้ไข
- สนับสนุนการมีส่วนร่วม
- ยกย่องการเสียสละ

7

## ส่งเสริมความบันเทิง อย่างสร้างสรรค์

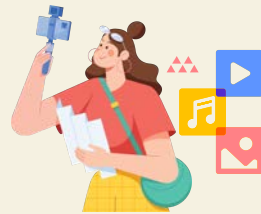


- เนื้อหาเหมาะสมกับวัย
- ส่งเสริมจินตนาการ
- พัฒนาทักษะต่าง ๆ
- สร้างความสนุกสนานผ่อนคลาย

## บทบาทสำคัญของผู้รับสาร ที่ช่วยให้สื่อหรือเนื้อหาเกิดประโยชน์กับสังคม

- คัดวิเคราะห์ แยกแยะข้อมูล
- ตรวจสอบความถูกต้อง
- เลือกบริโภคสื่อที่มีคุณภาพ
- แบ่งปันเนื้อหาดี ๆ
- ร่วมสร้างสรรค์เนื้อหาที่เป็นประโยชน์

# การสร้างเนื้อหาดิจิทัล ให้ดึงดูด และเกิดการจดจำ



ทุกวันนี้การสื่อสาร เทคโนโลยี และไอเดีย ทำให้ไม่ว่าใครก็สามารถเป็น Content Creator ได้ แต่การที่เราจะกลายเป็นคนสร้างเนื้อหาดิจิทัล เราต้องอย่าลืมคิดว่า เมื่อเรามีผู้ติดตาม เราจะกลายเป็นคนที่ส่งผลต่อแนวคิด และมีอิทธิพลต่อคนเหล่านั้น ดังนั้น ต้องคิดให้ดีกว่าเราจะนำเสนอเนื้อหาอะไร และอย่างไรจึงจะเหมาะสม

## แนวทางการสร้างเนื้อหา ให้ดึงดูด และเกิดการจดจำ

### 1) วิเคราะห์ให้รู้ว่ากลุ่มเป้าหมาย



สนใจอะไร ต้องการอะไร แล้วสร้างสื่อให้ตรงกับกลุ่มเป้าหมาย

### 2) เลือกหัวข้อที่น่าสนใจ



อาจจะเป็นหัวข้อที่ไม่น่าจะมีใครรู้มาก่อน หรือนำเสนอแง่มุมใหม่ที่คาดไม่ถึง

### 3) เขียนเนื้อหาให้ง่าย กระชับ



เนื่องจากผู้คนมีการจดจ่อกับสื่อใดสื่อหนึ่งน้อยลงมาก อีกทั้งยังมีสื่ออีกจำนวนมากให้เลือกดู หากเข้าใจยากไปคนอาจจะเปลี่ยนไปดูสื่ออื่น ๆ แทน

#### 4) ใส่ใจรูปภาพ 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

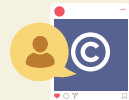
การสร้างเนื้อหาที่มีคุณภาพไม่เพียงให้ความสำคัญกับความน่าสนใจ และคุณค่าที่นำเสนอเท่านั้น แต่ยังต้องพิจารณาถึงจริยธรรม และการไม่ผิดต่อกฎหมายด้วย

### หลักการการสร้างเนื้อหาอย่างมีจริยธรรม และไม่ผิดกฎหมาย

1 **ชื่อสัตย์ต่อผู้ชม ไม่บิดเบือนข้อมูล**  
เพื่อให้ได้รับความสนใจ



2 **เคารพลิขสิทธิ์และทรัพย์สินทางปัญญา**  
ไม่แอบอ้างเอาผลงานของผู้อื่นมาเป็นของตัวเอง



3 **รับผิดชอบต่อสังคม**



4 **ป้องกันข้อมูลส่วนบุคคลของทุกคนที่เกี่ยวข้อง**



5 **ตรวจสอบข้อเท็จจริงก่อนเผยแพร่เนื้อหา**



6 **ให้เครดิตหรืออ้างอิงที่เหมาะสม**

ไม่ละเมิดลิขสิทธิ์ผู้อื่น หากมีส่วนที่นำเนื้อหา  
ของผู้อื่นมาใช้งาน



7 **หลีกเลี่ยงเนื้อหาที่ก่อให้เกิดความขัดแย้ง  
หรือปลุกกระดม**



## แนวทางปฏิบัติ

1

**ตรวจสอบข้อมูลก่อนนำมาเผยแพร่ :**

ตรวจสอบความถูกต้องของข้อมูล แหล่งที่มา และความน่าเชื่อถือ หลีกเลี่ยงการเผยแพร่ข่าวลือ ข้อมูลเท็จ หรือข้อมูลที่บิดเบือน

2

**อ้างอิงแหล่งที่มาของข้อมูล :**

ระบุแหล่งที่มาของข้อมูลอย่างชัดเจน เพื่อให้ผู้อื่นสามารถตรวจสอบข้อมูลย้อนหลังได้

3

**ระบุชื่อผู้สร้างเนื้อหา :**

ระบุชื่อผู้สร้างเนื้อหา ช่องทางการติดต่อ และข้อมูลอื่น ๆ ที่เกี่ยวข้อง

4

**หลีกเลี่ยงการใช้ภาษาที่รุนแรงหรือไม่เหมาะสม :**

ใช้ภาษาสุภาพ เหมาะสมกับกลุ่มเป้าหมาย หลีกเลี่ยงการใช้คำหยาบคาย ภาษาที่แสดงความเกลียดชังหรือภาษาที่สร้างความเสียหาย

5

**คิดวิเคราะห์และไตร่ตรองก่อนแชร์ต่อ :**

ตรวจสอบเนื้อหา ความถูกต้อง และความน่าเชื่อถือ ก่อนที่จะแชร์ต่อ

## กรณีศึกษา

1

**การเผยแพร่ข่าวลือ** : การเผยแพร่ข้อมูลเท็จหรือบิดเบือนความจริง อาจสร้างความเสียหายต่อบุคคลอื่นหรือสังคม

ตัวอย่างเช่น การเผยแพร่ข่าวลือเกี่ยวกับสถานการณ์โรคระบาด อาจสร้างความตื่นตระหนกและความหวาดกลัว

2

**การละเมิดลิขสิทธิ์** : การนำผลงานของผู้อื่นมาใช้โดยไม่ได้รับอนุญาต เป็นการละเมิดลิขสิทธิ์

ตัวอย่างเช่น การนำรูปภาพจากเว็บไซต์มาใช้โดยไม่ได้อনุญาต

3

**การปลุกระดมความเกลียดชัง** : การโพสต์ข้อความหรือรูปภาพที่สร้างความเกลียดชัง แบ่งแยก หรือดูหมิ่นบุคคลอื่น

ตัวอย่างเช่น การโพสต์ข้อความที่แสดงความเกลียดชังต่อบุคคลต่างศาสนา

## ตัวอย่างเครื่องมือและแหล่งข้อมูล

- **Creative Commons :**

องค์กรที่จัดทำสัญญาอนุญาตแบบเปิด ช่วยให้ผู้สร้างเนื้อหาสามารถกำหนดเงื่อนไขการใช้งาน

- **เว็บไซต์ของกรมทรัพย์สินทางปัญญา :**

ให้ข้อมูลเกี่ยวกับกฎหมายและวิธีการจดทะเบียนลิขสิทธิ์  
(<https://www.ipthailand.go.th/>)

- **เว็บไซต์ของสำนักงานคณะกรรมการกฤษฎีกา :**

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



# ลิขสิทธิ์ กับ CREATIVE COMMONS

## เรารู้จักลิขสิทธิ์ดีแค่ไหน ?

สื่อและเนื้อหาทุกอย่างล้วนมีลิขสิทธิ์ เราไม่สามารถนำมาใช้ได้ โดยไม่ขออนุญาตจากเจ้าของ การ Repost อาจดูเป็นเพียงการโพสต์ธรรมดา หยิบเรื่องเก่านำมาโพสต์ใหม่ เพื่อให้ผู้ติดตามหรือคนอื่น ๆ ที่ไม่เคยเห็น ได้เห็น เป็นการแชร์เรื่องราวดี ๆ ใหม่อีกครั้ง แต่ถ้าเราไม่ใช่คนที่คิดหรือสร้างเนื้อหานั้นขึ้นมาเอง ก็อาจกลายเป็นเรื่องของการละเมิดสิทธิ์ของผู้อื่นได้

## 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) โสตทัศนวัสดุ



เช่น คอมพิวเตอร์พร้อมหูฟัง เครื่องฉายวิดีโอโปรเจกเตอร์ เป็นต้น

#### 6) ภาพยนตร์



#### 7) สิ่งบันทึกเสียง



เช่น คอมพิวเตอร์พร้อมหูฟัง เครื่องบันทึกเสียง เป็นต้น

#### 8) งานแพร่เสียงแพร่ภาพ



เช่น รายการโทรทัศน์ เป็นต้น

#### 9) งานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ



เช่น การพิมพ์ศิลปะบนร่างกาย เป็นต้น

## ลิขสิทธิ์ กับ CREATIVE COMMONS ต่างกันอย่างไร ?



### ลิขสิทธิ์

คือ สิทธิ์ที่มีเพียงผู้เดียวที่จะสามารถกระทำต่อชิ้นงานที่มีลิขสิทธิ์



### Creative Commons (ครีเอทีฟ คอมมอนส์)

เป็นองค์กรไม่แสวงหากำไร ที่สนับสนุนการแบ่งปันงานสร้างสรรค์และข้อมูล ตามแนวทางการใช้งานและลิขสิทธิ์ในปัจจุบัน



### Creative Commons ทำงานร่วมกับ “ลิขสิทธิ์”

โดยเสนอทางเลือก ให้เจ้าของลิขสิทธิ์แบ่งปันการใช้งานลิขสิทธิ์ให้คนอื่น ในรูปแบบของสัญญาอนุญาตครีเอทีฟคอมมอนส์ (CC License) เป็นทางเลือกที่ยืดหยุ่นกว่าและตอบโจทย์ของเจ้าของลิขสิทธิ์แต่ละคนได้ตรงใจ



## ประเภทของสัญญาอนุญาต CC License

### 1. Attribution (BY)



สัญลักษณ์เพื่อรับรองสิทธิเจ้าของลิขสิทธิ์ อนุญาตให้ผู้อื่นนำเนื้อหาหรือผลงานไปใช้ได้ คนที่จะนำไปใช้ต้องรับรู้ถึงผู้ถือลิขสิทธิ์เสมอ ต้องอ้างอิงด้วยว่าเอามาจากไหน

### 2. Share Alike (SA)



สัญลักษณ์เพื่อรับรองสิทธิเจ้าของลิขสิทธิ์ อนุญาตให้ผู้อื่นนำเนื้อหาหรือผลงานไปใช้ได้ คนที่จะนำไปใช้ต้องรับรู้ถึงผู้ถือลิขสิทธิ์เสมอ ต้องอ้างอิงด้วยว่าเอามาจากไหน

### 3. Non-Commercial (NC)



อนุญาตให้ทำซ้ำ แจกจ่าย นำไปแสดงและดัดแปลงงานได้ แต่ไม่อนุญาตให้นำไปใช้เชิงพาณิชย์ หรือทางการค้า

### 4. No Derivative Works (ND)



ห้ามมีการดัดแปลงงาน ทำซ้ำ แจกจ่าย นำไปแสดงได้ เฉพาะงานตามต้นฉบับเดิมเท่านั้น

## 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 แต่ห้ามนำไปใช้แสวงหาผลกำไร

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



สามารถนำผลงานไปใช้ แสวงหาผลกำไรได้ ต้องให้เครดิตเจ้าของผลงาน และเผยแพร่เป็น CC License แบบเดียวกับต้นฉบับ

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



สามารถนำผลงานไปใช้ได้ ต้องให้เครดิตเจ้าของผลงาน แต่ห้ามนำไปแก้ไข ตัดแปลง รวมถึงใช้แสวงหาผลกำไร

## วิธีเช็คสิทธิ์สื่อ ก่อนนำมาใช้งาน

หลังจากเราได้ทราบแล้วว่า ผลงานที่ได้จากอินเทอร์เน็ตนั้นแบบไหน ใช้ได้หรือไม่ได้ เรามาดูสรุปเช็กลิสต์ลิขสิทธิ์การใช้สื่อ เพื่อความมั่นใจ และไม่ผิดกฎหมายกัน

### ใช้ได้



- สร้างสรรค์รูปภาพรูปนี้ขึ้นมาเอง
- ใช้ภาพของผู้อื่นเพื่อรายงานข่าว การศึกษา หรืองานวิจัย
- ใช้ภาพของผู้อื่นที่มี Creative Commons เพื่อการค้าหรือกำไรส่วนบุคคล โดยใช้ตามเงื่อนไขที่อนุญาต

### ใช้ไม่ได้



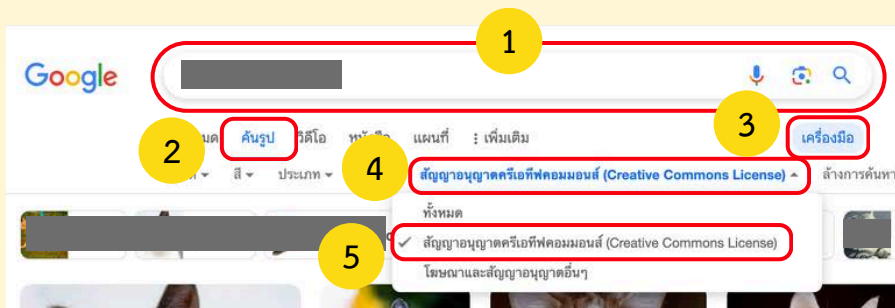
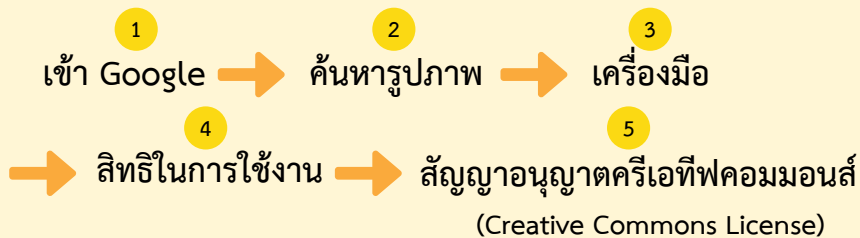
- ภาพของผู้อื่นที่ไม่ได้รับอนุญาตจากแหล่งต้นฉบับ
- ใช้ภาพของผู้อื่นเพื่อการค้าหรือกำไรส่วนบุคคล โดยไม่จ่ายเงินเพื่อใช้รูปภาพ

## วิธีการใช้งานรูปที่ได้รับการอนุญาต

# ง่าย ๆ จาก Google



ลองมาดูวิธีการง่าย ๆ ในการค้นหารูปบนอินเทอร์เน็ตที่ได้รับอนุญาต  
ให้นำไปใช้งานได้ ดังนี้



## กฎหมายที่เกี่ยวข้อง



### 1) กรณีละเมิดลิขสิทธิ์โดยตรง

การกระทำอย่างใดอย่างหนึ่งแก่งานอันมีลิขสิทธิ์โดยไม่ได้รับอนุญาต ได้แก่ ทำซ้ำหรือดัดแปลง และนำออกเผยแพร่ต่อสาธารณชน

มาตรา 69

ผู้ใดกระทำการละเมิดลิขสิทธิ์หรือสิทธิของนักแสดงตามมาตรา 271

มาตรา 282 มาตรา 293 มาตรา 304 หรือมาตรา 525

โทษ : ปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นการกระทำเพื่อการค้า ผู้กระทำต้องระวางโทษ จำคุกตั้งแต่หกเดือนถึงสี่ปี หรือปรับตั้งแต่หนึ่งแสนบาทถึงแปดแสนบาท หรือทั้งจำทั้งปรับ

### 2) กรณีละเมิดลิขสิทธิ์โดยอ้อม

การละเมิดโดยบุคคลใดรู้อยู่แล้ว หรือมีเหตุอันควรรู้อย่างใดได้ทำขึ้นโดยละเมิดลิขสิทธิ์ของผู้อื่น ซึ่งกระทำอย่างใดอย่างหนึ่งแก่งานนั้นเพื่อหากำไร

มาตรา 70 ผู้ใดกระทำการละเมิดลิขสิทธิ์ตามมาตรา 316

โทษ : ปรับตั้งแต่หนึ่งหมื่นบาทถึง หนึ่งแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นการกระทำเพื่อการค้า ผู้กระทำต้องระวางโทษ 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, วรัญญ. (2566). ความสำคัญของ Citation ในงานวิจัย. กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์.

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

**ตัวอย่าง :**

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

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

**ตัวอย่าง :**

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

**การอ้างอิงงานประเภทอื่นๆ**

- งานนำเสนอ :  
นามสกุล, ชื่อ. (ปีพิมพ์). ชื่อเรื่อง. ประชุมวิชาการ ชื่อประชุม, สถานที่จัดประชุม, วันที่จัดประชุม.
- รายงานการวิจัย :  
นามสกุล, ชื่อ. (ปีพิมพ์). ชื่อเรื่อง. ชื่อหน่วยงาน.
- วิทยานิพนธ์ :  
นามสกุล, ชื่อ. (ปีพิมพ์). ชื่อเรื่อง. วิทยานิพนธ์ (ระดับปริญญา), ชื่อมหาวิทยาลัย.

## การอ้างอิงในเนื้อหา

มี 2 วิธีหลักในการอ้างอิงในเนื้อหา

**1. การอ้างอิงแบบแทรกในเนื้อหา :**

เขียนชื่อผู้แต่งและปีที่พิมพ์ในวงเล็บกลม (Smith, 2023)

**2. การอ้างอิงแบบบรรณานุกรม :**

เขียนรายการอ้างอิงทั้งหมดไว้ท้ายงานวิจัย

## การจัดรูปแบบบรรณานุกรม

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

## ตัวอย่างการจัดรูปแบบบรรณานุกรม

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

## เครื่องมือช่วยอ้างอิง

มีเครื่องมือมากมายที่ช่วยในการอ้างอิง เช่น Zotero, Mendeley, EndNote ช่วยให้ผู้ใช้จัดการรายการอ้างอิง จัดรูปแบบการอ้างอิง และสร้างรายการอ้างอิงโดยอัตโนมัติ

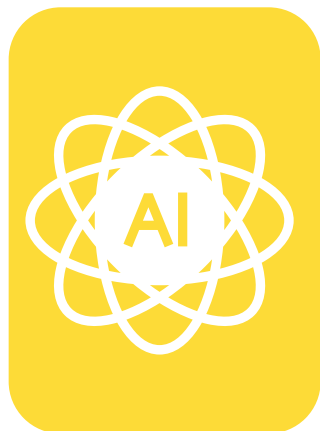
ข้อควรระวัง

- ตรวจสอบให้แน่ใจว่ารูปแบบการอ้างอิงถูกต้อง และสอดคล้องกันทั้งงานวิจัย
- อ้างอิงแหล่งที่มาทั้งหมดที่ใช้ในงานวิจัย
- หลีกเลี่ยงการลอกเลียนงานผู้อื่น





สื่อเนื้อหาดีจิตัลหลายรูปลักษณ  
 อยู่ที่ปีกความต้องการช่องทางชอบ  
 ดั่งนั้นผู้สร้างเนื้อหาต้องมีกรอบ  
 ทำรอบคอบถูกกฎหมายจริยธรรม  
 สร้างสรรค์งานควรเคารพลิขสิทธิ์  
 ใช้ความคิดไม่ลอกเลียนผลิตซ้ำ  
 ทุกงานเขียนงานสร้างวรรณกรรม  
 ให้เป็นธรรมกับเจ้าของต้องอ้างอิง



ถ้าคุณเรียนผ่านด้านนี้  
คุณจะสามารถเพิ่มพูนทักษะ  
ด้าน AI และใช้ประโยชน์  
ได้อย่างสูงสุด

# 5.3

## DATA & AI GOVERNANCE

### วัตถุประสงค์

1. ผู้เรียนสามารถอธิบายความหมาย ประเภท หลักการทำงานพื้นฐานของ AI ได้แก่ MACHINE LEARNING, NEURAL NETWORKS และ DEEP LEARNING ได้
2. ผู้เรียนมีความรู้เกี่ยวกับ การใช้งาน AI ที่เกี่ยวข้องในชีวิตประจำวัน รวมถึงการใช้ประโยชน์จาก AI อย่างมีธรรมาภิบาล
3. ผู้เรียนตระหนักถึงผลกระทบ ความเสี่ยง และแนวปฏิบัติที่ควร และไม่ควรทำในการใช้ AI อย่างมีธรรมาภิบาล

# เท่ากัน AI



## เทคโนโลยีเพื่ออนาคต

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

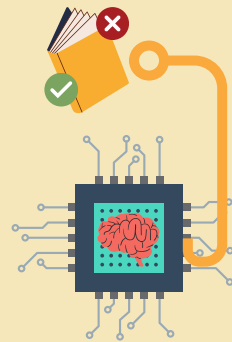
### ประเภทของ AI

แบ่งออกได้เป็น 3 ประเภทหลัก ได้แก่

#### 1. Machine Learning (ML)

เป็นสาขาหลักของ AI ที่ให้คอมพิวเตอร์มีความสามารถในการเรียนรู้จากข้อมูล โดยไม่ต้องมีโปรแกรมอย่างชัดเจน ทำงานโดยการวิเคราะห์ชุดข้อมูลใหญ่เพื่อค้นหารูปแบบ และความสัมพันธ์

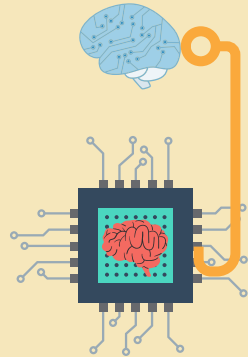
ประโยชน์ : ปรับปรุงความแม่นยำในการทำนายผลลัพธ์จากข้อมูลขนาดใหญ่



## 2. Neural Networks

มีการออกแบบโครงสร้าง ที่เลียนแบบเซลล์ประสาท ในสมองมนุษย์ ช่วยให้คอมพิวเตอร์สามารถจำแนก และตีความข้อมูลได้ซับซ้อน เช่น ภาพ เสียง เป็นต้น

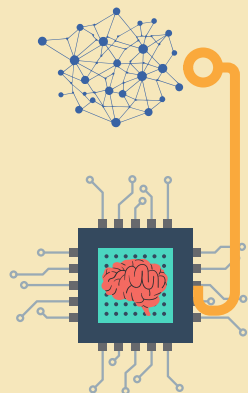
ประโยชน์ : ช่วยเพิ่มประสิทธิภาพในงานที่เกี่ยวข้องกับการจดจำและการประมวลผลภาพ



## 3. Deep Learning

เป็นส่วนขยายของ Neural Networks ที่ใช้ขั้นตอนการประมวลผลหลายชั้นเพื่อวิเคราะห์ข้อมูล ช่วยให้ระบบ AI สามารถเรียนรู้ความสัมพันธ์ที่ซับซ้อนได้เอง

ประโยชน์: สามารถจำแนกและทำนายข้อมูลได้อย่างแม่นยำสูง



# โอกาสและความท้าทาย จาก AI



ยุคของ AI นำมาซึ่งการเปลี่ยนแปลงหลายอย่าง เนื่องจากประโยชน์ของ AI นั้นส่งผลต่อการดำรงชีวิต เช่น

## 1 การแพทย์



มีส่วนช่วยหมอในการวินิจฉัยโรค หรือช่วยพัฒนาตัวยา

## 2 การศึกษา



มีส่วนในการพัฒนาหลักสูตร และช่วยให้การเรียนรู้มีประสิทธิภาพ

## 3 ด้านธุรกิจ



ช่วยวิเคราะห์ข้อมูลและเพิ่มประสิทธิภาพในการทำงาน

## 4 การคมนาคม



มีการพัฒนารถยนต์ไร้คนขับ และระบบขนส่งอัจฉริยะ

## ประเภทของความท้าทาย ในการใช้ประโยชน์จาก AI

### 1. ความกังวลเรื่องความเป็นส่วนตัว และความปลอดภัยของข้อมูล

การเก็บรวบรวมและการวิเคราะห์ข้อมูลขนาดใหญ่ที่ AI ต้องการอาจเป็นความเสี่ยงต่อความเป็นส่วนตัวของคุณ นอกจากนี้ ยังมีความเสี่ยงที่ข้อมูลนั้นอาจถูกใช้ในทางที่ผิดหรือถูกแฮ็กได้

### 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 รถไฟฟ้าไร้คนขับ เป็นต้น

### การซื้อขาย - ขายของออนไลน์

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

### ความบันเทิง

- แพลตฟอร์มสตรีมมิงวิดีโอ เช่น Netflix YouTube
- แอปพลิเคชันฟังเพลง เช่น Spotify Apple Music
- เกมที่ใช้ AI เช่น Dreamscaper The Sims

### สุขภาพและความเป็นอยู่ที่ดี

- อุปกรณ์ติดตามสุขภาพ เช่น Fitbit Apple Watch
- แอปพลิเคชันสำหรับติดตามการนอนหลับ
- แชทบอตสำหรับให้คำปรึกษาด้านสุขภาพ

## การศึกษา

- แพลตฟอร์มการเรียนรู้แบบออนไลน์ เช่น Khan Academy Coursera
- ระบบติวเตอร์อัจฉริยะ
- เทคโนโลยีการตรวจสอบการลอกเลียนแบบ

## ภาครัฐ

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



# การใช้ประโยชน์จาก AI อย่างมีธรรมาภิบาล

## ความหมายของ ธรรมาภิบาลใน AI

ธรรมาภิบาลใน AI หมายถึง การพัฒนาและการใช้งาน AI โดยคำนึงถึงหลักจริยธรรม ความโปร่งใส ความยุติธรรม และความรับผิดชอบ มีจุดมุ่งหมายเพื่อให้เทคโนโลยีนี้มีประโยชน์ต่อสังคมโดยรวมโดยไม่ส่งผลกระทบต่อบุคคลหรือกลุ่มคนใด

## การใช้ AI อย่างมีธรรมาภิบาล สำหรับคนทั่วไป

- เลือกใช้ผลิตภัณฑ์และบริการที่โปร่งใสและมีจริยธรรม

ก่อนตัดสินใจใช้ผลิตภัณฑ์ หรือบริการ AI ใด ๆ ควรศึกษาและทำความเข้าใจวิธีการทำงานของ AI เช่น แอปพลิเคชันที่แนะนำเนื้อหา โดยอาศัยระบบ Machine Learning หรือการเรียนรู้ของระบบ ควรมีนโยบายความเป็นส่วนตัว และการใช้ที่ชัดเจน เป็นต้น

- **ใช้งาน AI โดยคำนึงถึงความเป็นส่วนตัว ให้ความสำคัญกับการปกป้องข้อมูลส่วนบุคคล**

เช่น การจำกัดการเข้าถึงข้อมูลส่วนบุคคลบนอุปกรณ์สมาร์ทโฮม หรือ การปรับการตั้งค่าความเป็นส่วนตัวบนโซเชียลมีเดียที่ใช้ AI ในการแนะนำเนื้อหา

- **สนับสนุนและใช้ผลิตภัณฑ์ที่มีการพัฒนาอย่างยั่งยืน สนับสนุนบริษัทและองค์กรที่ใช้ AI เพื่อการพัฒนาที่ยั่งยืน**

เช่น การใช้ AI ในการปรับปรุงระบบพลังงาน การจัดการขยะ หรือ การเกษตรที่มีประสิทธิภาพ

- **มีส่วนร่วมในการสร้างความตระหนักรู้ และการศึกษาเกี่ยวกับ AI**

ใช้โอกาสในการศึกษาและส่งเสริมความตระหนักรู้ เกี่ยวกับ AI และ จริยธรรมในการใช้งาน เพื่อให้สังคมมีความเข้าใจ และสามารถใช้ เทคโนโลยีนี้ได้อย่างรับผิดชอบ

- มีส่วนร่วมในการตั้งคำถามและวิพากษ์วิจารณ์

เมื่อพบเห็นการใช้งาน AI ที่อาจนำไปสู่ความไม่เป็นธรรมหรือละเมิดจริยธรรม มีส่วนร่วมในการตั้งคำถามและวิพากษ์วิจารณ์ผ่านช่องทางต่าง ๆ เช่น โซเชียลมีเดีย หรือการรณรงค์



# ความเสี่ยงจาก การใช้เทคโนโลยี AI

ในขณะที่ปัญญาประดิษฐ์ (AI) เริ่มมีบทบาทสำคัญในหลายด้านของชีวิตและการทำงาน แต่ในทางกลับกันก็นำมาซึ่งความเสี่ยง และความท้าทายที่ไม่ควรมองข้าม

## ความเสี่ยงจากการใช้เทคโนโลยี AI

- ความเสี่ยงต่อความเป็นส่วนตัวและข้อมูล

หนึ่งในความเสี่ยงหลักของ AI คือ การละเมิดความเป็นส่วนตัว ระบบ AI ที่วิเคราะห์ข้อมูลส่วนบุคคลอาจเปิดโอกาสให้ข้อมูลนั้นถูกใช้งานอย่างไม่เหมาะสมหรือรั่วไหล ซึ่งสามารถนำไปสู่การละเมิดสิทธิส่วนบุคคลและความเสี่ยงด้านความปลอดภัยข้อมูล

- ความเสี่ยงต่อการเกิดอคติและการตัดสินใจที่ไม่ยุติธรรม AI

หาก AI ได้รับข้อมูลที่มาอคติมากเกินไป สามารถสร้างผลลัพธ์ที่ไม่ยุติธรรม โดยเฉพาะในการตัดสินใจที่เกี่ยวข้องกับการจ้างงาน การให้สินเชื่อ หรือการพิจารณาคดีทางกฎหมาย ซึ่งอาจนำไปสู่การเลือกปฏิบัติและความไม่เท่าเทียม

- **ความเสี่ยงต่อการสูญเสียงาน**

การอัตโนมัติที่ขับเคลื่อนโดย AI สามารถทำหน้าที่แทนมนุษย์หลายงาน นำไปสู่ความกังวลเรื่องการสูญเสียงานและความท้าทายในการทำงานใหม่สำหรับแรงงานในอุตสาหกรรมที่ได้รับผลกระทบ

- **ความเสี่ยงต่อความปลอดภัย AI**

มีความสามารถในการปรับปรุงระบบความปลอดภัย ในขณะเดียวกันก็สร้างความเสี่ยงใหม่ ๆ เช่น การใช้ AI ในการพัฒนา malware หรือการโจมตีทางไซเบอร์ที่ซับซ้อนขึ้น นอกจากนี้ AI ที่ควบคุมอาวุธหรือระบบสำคัญ อาจนำไปสู่ความเสี่ยง ที่ไม่สามารถคาดการณ์ได้ หากถูกใช้งานอย่างไม่เหมาะสม

- **ความเสี่ยงต่อการควบคุมที่ลดลง**

การพัฒนา AI ที่มีความสามารถสูงสุดอาจนำไปสู่สถานการณ์ที่มนุษย์ไม่สามารถควบคุมหรือทำความเข้าใจการตัดสินใจของระบบ AI ได้ เราต้องการกลไกในการตรวจสอบและควบคุม AI เพื่อให้แน่ใจว่ามันทำงานได้ตามวัตถุประสงค์และไม่สร้างความเสี่ยงที่ไม่คาดคิด

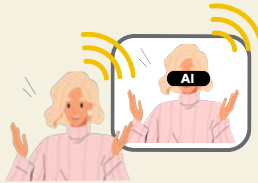


## TIP

## รวมรูปแบบของ AI ที่มีจลาชีพนำไปใช้

ตำรวจสอบสวนกลาง (CIB) ได้รวบรวมรูปแบบของ AI ที่มีจลาชีพนำมาใช้ ดังนี้

### - Voice Cloning



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

### - Deepfake



หรือการใช้ AI ปลอมแปลงใบหน้าให้มีความคล้ายคลึงกับบุคคลต่าง ๆ เพื่อหลอกเชื่อว่าคน ๆ นั้น ได้ทำแบบนั้นจริงหรือปลอมเป็นคนใกล้ตัวเพื่อหลอกเหยื่อให้หลงเชื่อ

**TIP**

- Fake Business หรือ การใช้ Generative AI ต่าง ๆ



ในการสร้างบทความ หรือสคริปต์วิดีโอเพื่อให้ดูเป็นมืออาชีพด้านต่าง ๆ เพื่อหลอกเหยื่อให้มาร่วมลงทุน หรือใช้ร่วมกันทั้ง 2 ข้อเพื่อความแนบเนียน

## วิธีป้องกันเบื้องต้น

- สังเกตจังหวะการเว้นวรรคคำพูด น้ำเสียง เสียงวรรณยุกต์

ว่ามีจังหวะเว้นวรรคตอนแปลกๆ หรือไม่ มีน้ำเสียงราบเรียบเกินไปไหม มีจังหวะหายใจใหม่ หรือออกเสียงวรรณยุกต์สูงต่ำ ผิดเพี้ยนหรือไม่

- หากเป็นคลิปวิดีโอ ที่ต้องสงสัย ให้สังเกตการขยับปาก

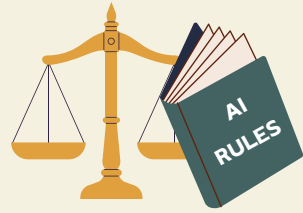
ของคนในคลิปว่าเป็นธรรมชาติหรือไม่ มีสัดส่วนผิดเพี้ยน หรือสีผิดๆ ต่าง ๆ หรือไม่ หรือมีการกระพริบตาถี่หรือน้อยเกินไปหรือไม่

**TIP**

- หากเป็นการวิดีโอคอล แล้วคนที่โทรมาดูแปลกไปจากเดิม ให้ลองถามคำถามเรื่องส่วนตัวที่มีแต่คนในครอบครัวเท่านั้นที่รู้ดูก่อน หากปลายทางตอบไม่ได้ ให้สันนิษฐานไว้ก่อนว่าเป็นมิจฉาชีพ
- ก่อนโอนเงิน หรือ ทำธุรกรรมใด ๆ ให้สังเกตชื่อบัญชี ก่อนโอนทุกครั้ง  
ว่าตรงกันกับบัญชีที่เราจะโอนหรือไม่ หากโดนบอกให้จ่ายค่าสินค้าให้ก่อน ให้ลองปฏิเสธก่อน ห้ามโอนไปที่ร้านโดยตรง เพราะอาจเป็นการโอนเข้าบัญชีม้า หรือบัญชีมิจฉาชีพได้
- สุดท้ายมีสติเสมอ  
หรือคิดให้รอบคอบก่อนที่จะตัดสินใจหลงเชื่อ หรือโอนเงิน

**ขอบคุณข้อมูล :** กองบัญชาการตำรวจสอบสวนกลาง

# Do / Don't ในการใช้ AI



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

## Do (ควรทำ)



- **ศึกษาและเข้าใจ AI :**

ใช้เวลาศึกษาเกี่ยวกับ AI และวิธีการทำงานของมัน เข้าใจถึงข้อจำกัดและศักยภาพของเทคโนโลยี

- **ปกป้องข้อมูลส่วนบุคคล :**

ใช้การตั้งค่าความเป็นส่วนตัวและระมัดระวังในการให้ข้อมูลส่วนบุคคลกับแอปพลิเคชันหรือบริการที่ใช้ AI

- **ใช้ AI เพื่อเพิ่มประสิทธิภาพ :**

ใช้ AI เพื่อเพิ่มประสิทธิภาพในการทำงานและชีวิตประจำวัน เช่น การใช้ AI ในการจัดการกับอีเมลหรือการจัดตารางงาน

- **ใช้ AI อย่างมีจริยธรรม :**

สนับสนุนและใช้ผลิตภัณฑ์ AI ที่ถูกพัฒนาอย่างมีจริยธรรมและโปร่งใส

# Don't

## (ไม่ควรทำ)



- อย่าละเลยความเป็นส่วนตัว :

อย่าละเลยการตั้งค่าความเป็นส่วนตัวหรือให้ข้อมูลส่วนบุคคลกับแอปพลิเคชันหรือบริการ โดยไม่ได้ตรวจสอบเงื่อนไขและนโยบายความเป็นส่วนตัว

- อย่าเชื่อมั่น AI อย่างสมบูรณ์ :

อย่าเชื่อมั่นในผลลัพธ์จาก AI อย่างไม่มีข้อสงสัย ควรมีการตรวจสอบและวิเคราะห์ข้อมูลด้วยตนเอง

- อย่าใช้ AI โดยไม่คำนึงถึงผลกระทบ :

อย่าใช้ AI ในวิธีที่อาจนำไปสู่ผลกระทบทางลบต่อผู้อื่นหรือสังคม โดยไม่ได้พิจารณาถึงความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้น

- อย่าลืมนการพัฒนาทักษะของตนเอง :

อย่าพึ่งพา AI อย่างเดียวในการทำงาน หรือการตัดสินใจ ควรพัฒนาทักษะและการเรียนรู้อย่างต่อเนื่องเพื่อทำงานร่วมกับ AI ได้อย่างมีประสิทธิภาพ

**TIP**

## การเขียน Prompt ทักษะใหม่ที่คุณควรใช้ในการใช้ AI อย่างมีประสิทธิภาพ



### Prompt คืออะไร ?

คือ คำสั่ง หรือชุดคำสั่งที่มนุษย์ป้อนให้กับ AI เพื่อกระตุ้นให้ AI สร้างผลลัพธ์ที่ต้องการ ไม่ว่าจะเป็น การสร้างข้อความ รูปภาพ โค้ด หรือการกระทำอื่น ๆ Prompt เปรียบเสมือนสะพานเชื่อมระหว่างความคิดของมนุษย์กับความสามารถของ AI ในการประมวลผล 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 ช่วยในการวิเคราะห์ข้อมูล รวมถึงการตัดสินใจ หรือแม้แต่ในการสื่อสารกับลูกค้าทางธุรกิจด้วย

### Prompt กับประโยชน์ในการบริหารจัดการ



นอกจากนี้ Prompt ยังสามารถใช้ในการสร้างรายงาน การวิเคราะห์ผลการทำงาน หรือแม้แต่เป็นตัวช่วยในการสร้างแผนการตลาด ช่วยให้การทำงานของเรและทีมงานเป็นเรื่องที่ง่าย และรวดเร็วยิ่งขึ้น

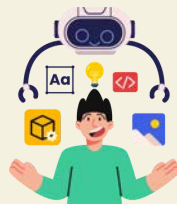
### Prompt กับประโยชน์ในการศึกษา



สำหรับนักเรียนนักศึกษา หรือผู้ที่สนใจใน AI การใช้ Prompt ที่ดีสามารถช่วยให้สามารถนำ AI ไปใช้ค้นหาข้อมูลในการเรียนรู้ และทำความเข้าใจบทเรียนได้ง่ายขึ้น รวมถึง ช่วยในการวิเคราะห์ข้อมูล เพื่อทำรายงานหรือสรุปบททวนบทเรียน

**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 แล้วเราจึงกำหนดบทบาทตามหน้าที่ที่สามารถทำได้ 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 และสร้างอะไร เพื่ออะไร 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

**TIP**

#### 4. ใช้ภาษาที่กระชับ ชัดเจน และเป็นธรรมชาติ

หลีกเลี่ยงการใช้คำศัพท์ที่กำกวม หรือประโยคที่ซับซ้อนเกินไป ใช้ภาษาที่เป็นธรรมชาติ เหมือนกับที่ใช้สื่อสารกับคนทั่วไป

#### 5. ระบุรูปแบบผลลัพธ์

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

#### 6. จำกัด Scope ของข้อความ

การจำกัด Scope ของงานให้เป็นที่เราต้องการ ทั้งการจำกัดจำนวนคำในข้อความ และการระบุเป้าหมายหลักที่ต้องการจะนำไปเผยแพร่ เช่น ต้องการจำกัดให้ผลลัพธ์ออกมาอยู่ภายใน 2,000 คำ และเน้นว่าให้เหมาะกับการทำการตลาดแบบออนไลน์ เป็นต้น

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

หากเป็นไปได้ ให้ยกตัวอย่างสิ่งที่ต้องการ เพื่อให้ AI เข้าใจรูปแบบที่ต้องการได้ง่ายขึ้น ตัวอย่างสามารถเป็นข้อความ รูปภาพ หรือโค้ดก็ได้

**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** เขียนบทความเกี่ยวกับประโยชน์ของการออกกำลังกายสำหรับผู้สูงอายุ ความยาวประมาณ 500 คำ ใช้ภาษาที่เข้าใจง่าย และเป็นกันเอง เน้นให้ข้อมูลที่เป็นประโยชน์และน่าเชื่อถือ

# อนาคตของ AI



## AI จะแทนที่งานมนุษย์หรือไม่ ?

AI จะแทนที่งานบางประเภท แต่ก็สร้างงานใหม่ ๆ ขึ้นมา ทักษะสำคัญสำหรับอนาคต 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) แหล่งเรียนรู้แบบออฟไลน์

- มหาวิทยาลัย : หลายมหาวิทยาลัยในประเทศไทยมีหลักสูตรเกี่ยวกับ AI
- งานสัมมนาและเวิร์กช็อป : มีการจัดงานสัมมนาและเวิร์กช็อปเกี่ยวกับ 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) ฟอรัมและชุมชนออนไลน์

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

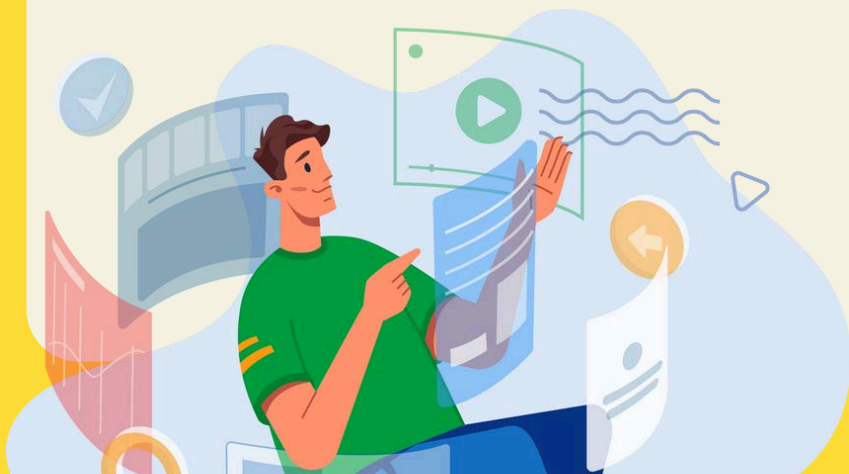
## อนาคตของ AI คืออะไร ?

**อนาคตของ AI  
มีแนวโน้มที่จะเติบโต  
และมีบทบาทมากขึ้นในสังคม**



การพัฒนา AI ที่มีธรรมาภิบาล การควบคุมและการกำกับดูแลที่เหมาะสมจะเป็นสิ่งสำคัญ ในการใช้ประโยชน์จากเทคโนโลยีนี้ให้ได้มากที่สุด ในขณะเดียวกัน ก็ต้องระมัดระวังความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

การใช้ AI ย่อมตามมาด้วยความรับผิดชอบ การตระหนักรู้และความเข้าใจ เพื่อให้สุดท้ายเราสามารถนำเทคโนโลยีนี้ไปใช้เพื่ออนาคตที่ดี ได้อย่างแท้จริง





บทส่งท้าย ให้ชวนคิด พิศ “เอไอ”  
 เท่าทันไว้ ใช้ได้เลิศ ก่อเกิดผล  
 ช่วยเขียนวาด Gen-สร้าง-เสริม เพิ่มพูนล้ำ  
 พัฒนา ฝึกฝน Prompt กลุ่มมกลไก  
 แต่อย่าเพิง รับทุกเมื่อ เชื่อทุกสิ่ง  
 ยิ่งดูจริง ยิ่งต้องตรวจ เข้มงวดไว้  
 ลับทักษะ ตระหนักรู้ คู่เอไอ  
 ใช้ปลอดภัย รับผิดชอบ รอบคอบเอย

รู้เท่าทันดิจิทัล  
ทักษะจำเป็น  
เพื่อชีวิตออนไลน์

# 5.1 Media & Information

แหล่งข้อมูลดิจิทัล

รูปแบบของ  
แหล่งข้อมูลดิจิทัล

เกณฑ์แบ่งประเภท  
แหล่งข้อมูลดิจิทัล

ประโยชน์ของ  
แหล่งข้อมูลดิจิทัล

ตัวอย่าง  
แหล่งข้อมูลดิจิทัล

การเลือกใช้งาน  
แหล่งข้อมูลดิจิทัล

หลักการเข้าถึง  
แหล่งข้อมูลดิจิทัล

แนวทางการรับชมสื่อ  
อย่างรู้เท่าทัน

ตระหนักถึง  
ธรรมชาติของสื่อ

ตรวจสอบ  
แหล่งที่มาของข้อมูล

ใช้วิจารณญาณ  
ในการรับชมสื่อ

ไม่ควรรับชมสื่อ  
จากแหล่งเดียว

มีส่วนร่วมในการ  
แลกเปลี่ยนข้อมูล

## 5.1

ธรรมชาติของสื่อ

ประเภทของ  
ธรรมชาติของสื่อ

สื่อ คือ สิ่งที่ถูก  
สร้างขึ้นมาจากมนุษย์

สื่อส่วนใหญ่ที่มี  
เป้าหมายธุรกิจ

สื่อสร้างค่านิยม  
และอุดมคติ

สื่อทำให้เกิดผล  
ทางการเมืองและสังคม

สื่อมีเอกลักษณ์  
และข้อจำกัดเฉพาะตัว

การกระทำ /  
พฤติกรรม

ผลกระทบ  
ทางกฎหมาย

ผลกระทบ  
ทางจริยธรรม

การประเมินคุณภาพ  
และความน่าเชื่อถือ  
ของข้อมูลจากสื่อดิจิทัล

ปัจจัยที่ใช้พิจารณา  
การประเมินคุณภาพ /  
ความน่าเชื่อถือของข้อมูล

รู้เท่าทัน Fake News

ประเภทของข้อมูลเท็จ

การตรวจสอบเบื้องต้น

สาเหตุที่มาของข้อมูลเท็จ

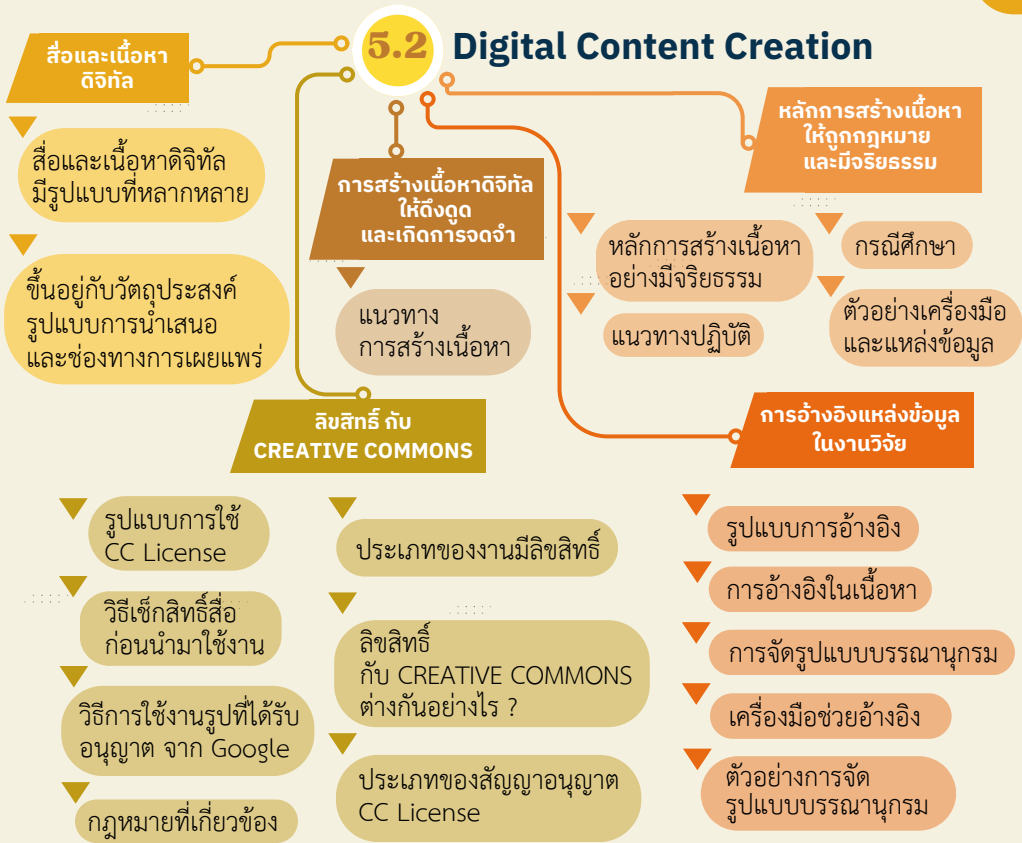
ศิลปะแห่งการจัดการ  
ข้อมูลจากสื่อดิจิทัล  
ด้วยตนเอง

แนวทางการจัดการข้อมูล

ผลจากการแบ่งปัน  
เนื้อหาที่ไม่เหมาะสม

ข้อมูลใดบ้าง ที่ทำบนโลกดิจิทัล  
แล้วขัดต่อกฎหมาย/จริยธรรม

## 5.2 Digital Content Creation



## 5.3 Data & AI Governance



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

ดวงรัตน์ วังเกล็ดแก้ว. (2564). 6 สัญญาณ ที่บอกว่าลูกกำลังเสพติดสื่อออนไลน์. สืบค้นเมื่อ 5 มิถุนายน 2567, จาก <https://citly.me/X9ePm>

เตือนภัยคนโสด ระวังถูกหลอกให้รักแล้วโอนเงิน. (2567, กุมภาพันธ์ 15). **Thairath Money**. [https://www.thairath.co.th/money/economics/thailand\\_econ/2763359](https://www.thairath.co.th/money/economics/thailand_econ/2763359)

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

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

- โรมัส กวาดามูช, วรวลัญช์ วัชรวรวัลย์ และ ณัฐริชต์ สาเมาะ. (2566). **ภูมิคุ้มกันในโลกดิจิทัล (Digital Resilience) ทักษะที่เด็กและเยาวชนไทยยุคใหม่ต้องมี.** สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://citly.me/5PbXx>
- บริษัท ดิทโต (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). **ทำความเข้าใจกับ Information Disorder “ความผิดปกติของข้อมูลข่าวสาร”** สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://citly.me/BrKWD>
- พีรพล อนุตรโสทธิ และ เจษฎา ศาลาทอง. (2564). **คู่มือภาคปฏิบัติ นักตรวจสอบข้อเท็จจริง (FACT-CHECK in ACTION).** พิมพ์ครั้งที่ 2. กรุงเทพฯ: คณะนิเทศศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.
- ภูษิษฐ์ อรัญพูล. (2567). **‘No.1 คือการสื่อสาร’ ทักษะที่นายจ้างต้องการมากที่สุด และ Soft Skill อะไรบ้างที่มั่งลงในปี 2024.** สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://www.blockdit.com/posts/66544213f864a30fba993157>
- ศิริกร เอื้อไพจิตร. (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 ลวงให้เชื่อ หลอกให้แชร์.** สืบค้นเมื่อ 6 มิถุนายน 2567, จาก <https://www.etcha.or.th/th/Useful-Resource/knowledge-sharing/articles/IFBL/FakeNews.aspx>
- สุวัชรียา จันทร์บัว. (2566, เมษายน 1). **ศูนย์ข่าวก่อนแชร์ สำนักข่าวไทย อสมท.** <https://tna.mcot.net/sureandshare-1145927>
- เสาวภาคย์ รัตนพงศ์. (2567, มีนาคม 28). **ศูนย์ข่าวก่อนแชร์ สำนักข่าวไทยอสมท.** <https://tna.mcot.net/sureandshare-1342212>
- อุกฤษฏ์ ตั้งสีบกกุล และ ปวีวัตร 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/iphone/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/marketing/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.เผยคนไทยออนไลน์ 7 ชั่วโมง 25 นาที 89.5% เข้าถึงอินเทอร์เน็ต.** สืบค้นเมื่อ 13 มิถุนายน 2567, จาก <https://mgronline.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](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? ทำไม HR ใช้คัดเลือกพนักงานได้.** สืบค้นเมื่อ 6 มิถุนายน 2567, จาก [https://th.hrnote.asia/recruit/digital-footprint-210630/#12\\_Digital\\_Footprint\\_HR](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](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



สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

อัจฉราพร หมุตระเด่น

กริช ขาวอุบลัมภ์

ชนนิกานต์ คงสุวรรณ

จิรายุทธ์ กุลพฤกษ์

นภาพร สีสาอด

### ที่ปรึกษา



ผศ.ดร.เจษฎา ศาลาทอง

คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ดร.ปรีชญ์ สง่างาม

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยมหิดล

ดร.ดารุวรรณ ศรีแก้ว

คณะครุศาสตร์อุตสาหกรรมและเทคโนโลยี  
มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าธนบุรี

นิธิภัทร ศรีธัญญา

ผู้อำนวยการสถาบันพัฒนาบุคลากรดิจิทัล

สถาบันพัฒนาบุคลากรดิจิทัล กรมพัฒนาฝีมือแรงงาน กระทรวงแรงงาน



### กองบรรณาธิการ



ศุภณัฏฐ์ก่อนแซร์ บริษัท อสมท จำกัด (มหาชน)

พีรพล อนุตรโสทธิ

จิรัชยา นวลนันทน้อย

อัครมณี ระวีแสงสุรย์

ยศวดี จิตบรรรศรีมี

จิราภา อ่อนเกลี้ยง

จิราพัชร สุวรรณพันธ์

กฤษณา กาญจนเพ็ญ

เสาวภาคย์ รัตน์พงศ์

ชยานิษฐ์ ผ่องใส

กัลย์ธีรา ตันเสถียร

ณัฐพล อินทร์สวัสดิ์

เบญญาภา วรรณระชีฟ

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

     : ETDA THAILAND



## สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

โทรศัพท์ : 02 123 1234 | โทรสาร : 02 123 1200



: ETDA THAILAND

