

# สังคมไทยในยุคดิจิทัล

รายวิชาสังคมไทยในยุคดิจิทัล

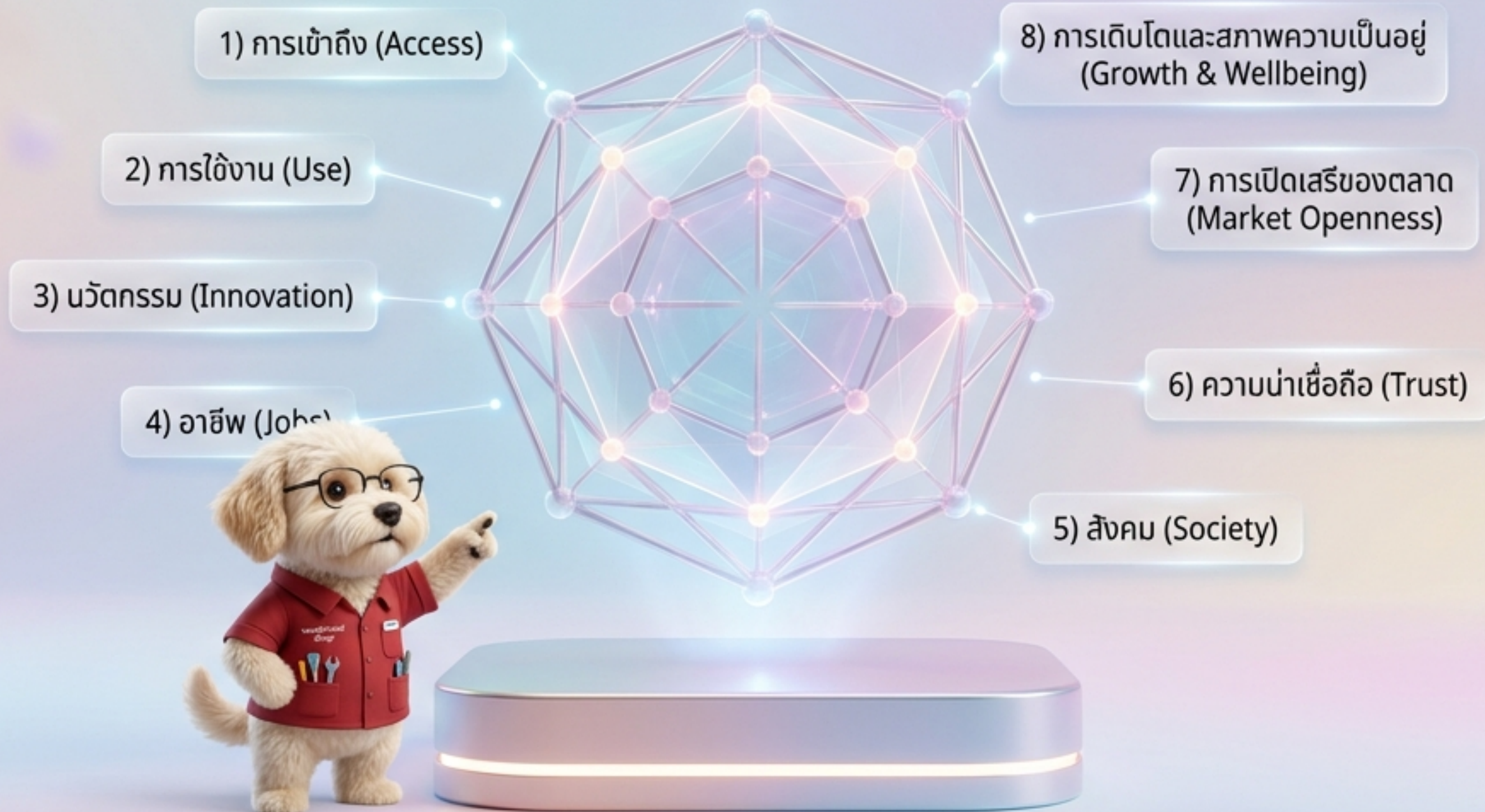
วิทยาลัยเทคนิคเขมราฐ

ผู้สอน นางสาวเจียรระโน กาญจนะโกมล (ครูเจีย)



# ภาพรวมดิจิทัลไทย: ก้าวหน้าต่อเนื่องใน 8 มิติ

ข้อมูลจากโครงการ Thailand Digital Outlook ปี 2568 (สำรวจกลุ่มตัวอย่างกว่า 46,625 ราย)  
ชี้ให้เห็นว่าเศรษฐกิจและสังคมดิจิทัลไทยขับเคลื่อนผ่าน 8 มิติหลัก:



# เศรษฐกิจยุคใหม่: สังคม “ลด” เงินสด (Less Cash) ไม่ใช่ “ไร้” เงินสด (Cashless)

Stone 1: Inception (ไทยกำลังอยู่ที่นี้)  
ยังพึ่งพาเงินสดสูง แต่เริ่มใช้ e-Payment

Stone 2: Tipping Point  
จุดเปลี่ยนผ่านพฤติกรรม

Stone 3: Transition  
โอนถ่ายสู่ระบบดิจิทัล

Stone 4: Advanced  
สังคมไร้เงินสดเต็มรูปแบบ  
(เช่น สวีเดน)



**ความจริงของสังคมไทย:**  
ปริมาณเงินสดหมุนเวียน (CIC)  
ต่อ GDP ของไทยยังคงตัวที่ร้อยละ 9.1  
แม้ e-Payment จะเติบโตแบบก้าวกระโดด  
(Exponential Growth)

# วิกฤตอาชญากรรมไซเบอร์: ลบความเชื่อผิดๆ เรื่อง "เหยื่อ"

ความเชื่อ:  
เหยื่อคือผู้สูงอายุ



ความจริง:  
วัยทำงานตกเป็นเหยื่อสูงสุด



สถิติคดีออนไลน์<sup>1</sup>  
(ปี.ค. 65 - ปี.ย. 68):  
955,723 คดี  
เสียหาย 93,685 ล้านบาท  
เฉลี่ยวันละ 785 คดี

ใครคือเหยื่อตัวจริง?:<sup>2</sup>  
อันดับ 1 คือ วัยทำงาน (อายุ 31-40 ปี)  
ร้อยละ 29.11  
อันดับ 2: อายุ 41-50 ปี (ร้อยละ 20.52)  
เพศ: หญิงตกเป็นเหยื่อถึง 64%



## Synthesis Insight

ผู้ใช้งานเทคโนโลยีจำนวนมาก มักมีความรู้ด้านความปลอดภัย (Cyber Security Awareness) ต่ำกว่าที่ตนเองคิด

# ทฤษฎีสามเหลี่ยมอาชญากรรม (The Crime Triangle)

## 1.เหยื่อหรือเป้าหมายที่เหมาะสม (Suitable Target)

คนที่มีมูลค่า, เข้าถึงง่ายทางออนไลน์, และขาดการระมัดระวังตัว

## 2. ผู้กระทำผิดที่มีแรงจูงใจ (Motivated Offender)

องค์กรอาชญากรรมข้ามชาติ, แฮกเกอร์ ที่ทำงานเป็นระบบเพื่อหวังผลตอบแทนทางการเงินสูงแต่ความเสี่ยงต่ำ

## 3. การขาดผู้พิทักษ์ (Absence of Capable Guardian)

ขาดระบบป้องกันภัยทางเทคนิค, ขาดความรู้เท่าทัน, หรือช่องว่างของการบังคับใช้กฎหมาย

### Core Concept

อาชญากรรมจะเกิดขึ้นได้ ต้องมีองค์ประกอบทั้ง 3 ประการในเวลาและพื้นที่ (ไซเบอร์) เดียวกัน

# ตัดวงจรอาชญากรรมไซเบอร์ด้วย ‘ผู้พิทักษ์ที่เข้มแข็ง’



## 1. สร้างความเข้มแข็งให้เหยื่อ (Empower Targets)

บูรณาการความรู้ด้านความปลอดภัยไซเบอร์ (Cybersecurity) เข้าสู่ระบบการศึกษาและผู้ใช้งาน

## 2. เพิ่มความเสี่ยงให้อาชญากร (Increase Risks)

เปลี่ยนจากการสืบสวนเชิงรับ (รอให้เกิดเหตุ) ไปสู่การบังคับใช้กฎหมายเชิงรุก (Proactive Law Enforcement)

## 3. ผู้พิทักษ์ที่เป็นองค์กร (Capable Guardians)

การทำงานไร้รอยต่อระหว่างภาครัฐ สถาบันการเงิน และภาคเอกชน เพื่ออายัดและสกัดกั้นเส้นทางเงินทันที

Core Concept

อาชญากรรมจะหยุดชะงักได้  
เมื่อสร้างระบบผู้พิทักษ์ที่มีประสิทธิภาพ ตัดวงจรได้ทันที

# กฎหมาย PDPA: เกราะป้องกันสิทธิความเป็นส่วนตัว

พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (บังคับใช้ 1 มิ.ย. 2565)  
มุ่งคุ้มครองและกำหนดมาตรฐานการใช้ข้อมูล



## ข้อมูลส่วนบุคคล (Personal Data)

ข้อมูลที่ระบุตัวตนได้ทั้งทางตรงและอ้อม  
(ไม่รวมคนตาย/นิติบุคคล)

**ตัวอย่าง:** ชื่อ-สกุล, เลขบัตร ปชช., เบอร์โทร, IP Address, Cookie ID, ลายนิ้วมือ, รูปภาพใบหน้า

## ข้อมูลที่มีความละเอียดอ่อน (Sensitive Data)

ข้อมูลที่ต้องระวังขั้นสูงสุด ห้ามเก็บหาก  
ไม่ได้รับความยินยอมชัดเจน

**ตัวอย่าง:** เชื้อชาติ, ศาสนา, ความคิดเห็นทางการเมือง, รสนิยมทางเพศ, ข้อมูลสุขภาพ, ประวัติอาชญากรรม

# 3 เสาหลักในระบบนิเวศของ PDPA



## เจ้าของข้อมูล (Data Subject)

**คือใคร:** บุคคลที่ข้อมูลสามารถระบุไปถึงได้  
(เช่น ตัวเรา ลูกค้า นักศึกษา)

**บทบาท:** มีสิทธิขอเข้าถึง แก้ไข ลบ  
หรือยกเลิกความยินยอมการใช้ข้อมูล



## ผู้ควบคุมข้อมูล (Data Controller)

**คือใคร:** บุคคล/นิติบุคคลที่มี "อำนาจตัดสินใจ"  
ในการเก็บ ใช้ หรือเปิดเผยข้อมูล

**บทบาท:** ต้องขอความยินยอม และรับผิดชอบ  
ตามกฎหมายหากข้อมูลรั่วไหล



## ผู้ประมวลผลข้อมูล (Data Processor)

**คือใคร:** บุคคล/นิติบุคคลที่ทำงาน "ตามคำสั่ง"  
ของผู้ควบคุมข้อมูล

**บทบาท:** ทำหน้าที่ประมวลผลข้อมูลตามสัญญา  
โดยไม่มีอำนาจตัดสินใจเอง

# บทลงโทษเมื่อละเมิด PDPA

## ทางปกครอง (Administrative Liability)

โทษปรับสูงสุดไม่เกิน 5 ล้านบาท  
(ขึ้นอยู่กับความร้ายแรงของการกระทำและประเภทของข้อมูล)

## ทางแพ่ง (Civil Liability)

ชดเชยค่าสินไหมทดแทนตามความเสียหาย  
ที่เกิดขึ้นจริง และศาลอาจสั่งปรับเพิ่ม  
(Punitive Damages) ได้สูงสุดอีก  
2 เท่าของค่าเสียหายจริง

## ทางอาญา (Criminal Liability)

โทษจำคุกสูงสุดไม่เกิน 1 ปี  
หรือปรับสูงสุดไม่เกิน 1 ล้านบาท  
หรือทั้งจำทั้งปรับ

# การเปลี่ยนผ่านเชิงโครงสร้างและ "วิกฤตวัฒนธรรม"



## เทคโนโลยีไร้พรมแดน

การเชื่อมโยงระดับโลก (Globalization)  
นำพาวิถีชีวิตข้ามชาติไหลบ่าเข้าสู่  
สังคมไทยอย่างรวดเร็ว



## เปลี่ยนผ่านสู่แพลตฟอร์ม

โครงสร้างการทำงาน เศรษฐกิจ  
และพฤติกรรมผู้บริโภค  
ถูกกำหนดโดยแพลตฟอร์มดิจิทัล



## ผลกระทบทางวัฒนธรรม

เกิดอัตลักษณ์ที่ถูกครอบงำ  
วัฒนธรรมดั้งเดิมกลายเป็นเพียง "สินค้า"  
นำไปสู่ปัญหาความเปราะบางทางจิตใจ  
สังคมปัจเจกชนนิยม และการสูญเสีย  
แก่นสารทางวัฒนธรรม

# ช่องว่างทางดิจิทัล (The Digital Divide): วิกฤตความเหลื่อมล้ำ

กลุ่มวัยรุ่นและวัยทำงาน  
(อายุ 15-39 ปี)  
อัตราการเข้าถึงอินเทอร์เน็ตสูงถึง  
**98.5% - 99.1%**  
(แทบจะสมบูรณ์แบบ)

กลุ่มผู้สูงอายุ  
(อายุ 60 ปีขึ้นไป)  
อัตราการเข้าถึงอินเทอร์เน็ตอยู่  
ที่เพียง **57.7%**

คีย์สำคัญ: “ช่องว่างทางดิจิทัล” คือความเหลื่อมล้ำระหว่างกลุ่มคนที่ได้ประโยชน์จากเทคโนโลยี กับกลุ่มคนที่ถูกทิ้งไว้ข้างหลังเนื่องจากข้อจำกัดทางกายภาพและทักษะ

# ผลกระทบเมื่อรัฐก้าวสู่ Digital Transformation

## บริการพื้นฐานของรัฐเปลี่ยนไป

นโยบาย สิทธิสวัสดิการ  
และการลงทะเบียนต่างๆ  
ย้ายไปอยู่บนระบบออนไลน์

## การสูญเสียโอกาส (Loss of Access)

ผู้สูงอายุที่ไม่มีอุปกรณ์ดิจิทัลหรือขาดทักษะ  
จะไม่สามารถเข้าถึงข่าวสาร สวัสดิการ  
หรือแม้แต่บริการทางสาธารณสุขได้

## ความเหลื่อมล้ำซ้อนทับ

ความเหลื่อมล้ำทางดิจิทัล  
นำไปสู่ความเหลื่อมล้ำทาง  
เศรษฐกิจและสังคมที่ลึกซึ้งยิ่งขึ้น



# บทสรุป: การอยู่รอดและเติบโตใน "สังคมไทยยุคดิจิทัล"

## Tech Adoption (เศรษฐกิจและนวัตกรรม)

ใช้ประโยชน์จาก e-Payment, แพลตฟอร์ม, และ AI เพื่อขับเคลื่อนการทำงานและยกระดับคุณภาพชีวิต

## Protective Awareness (ภูมิคุ้มกันไซเบอร์ & กฎหมาย)

เป็น "ผู้พิทักษ์" ที่เข้มแข็ง รู้ทันอาชญากรรม (Crime Triangle) และเคารพสิทธิความเป็นส่วนตัวตามกฎหมาย (PDPA)

## Cultural Core (อัตลักษณ์และจริยธรรม)

รักษาแก่นแท้ของความกตัญญูและวิถีไทย รู้จักประยุกต์ใช้วัฒนธรรมข้ามชาติโดยไม่สูญเสียตัวตนเพื่อป้องกันวิกฤตความเปราะบางทางจิตใจ



กุญแจสำคัญคือ "ความสมดุล" (Balance)  
ระหว่างความก้าวหน้าทางเทคโนโลยีและความมั่นคงของมนุษย์