

ความเสี่ยงของ AI พร้อมแนวทางการใช้งานอย่างปลอดภัยในยุคดิจิทัล

1 ความเป็นส่วนตัวและข้อมูลส่วนบุคคล



ปัญหาการละเมิดข้อมูล: AI มักต้องใช้ข้อมูลจำนวนมากในการประมวลผล ซึ่งอาจทำให้ข้อมูลส่วนบุคคลของผู้ใช้รั่วไหลได้

แนวปฏิบัติ: ควรตรวจสอบนโยบายความเป็นส่วนตัวของแพลตฟอร์มที่ใช้ AI และป้องกันข้อมูลส่วนตัว เช่น การไม่ให้สิทธิ์เข้าถึงข้อมูลที่ไม่จำเป็น

2 ความปลอดภัยและความน่าเชื่อถือของระบบ



ข้อผิดพลาดของ AI: แม้ AI จะมีความแม่นยำ แต่ก็ยังอาจทำผิดพลาดได้ เช่น การวินิจฉัยโรคผิดพลาด หรือข้อเสนอแนะที่ไม่ถูกต้อง

แนวปฏิบัติ: ใช้ AI เป็นเพียงเครื่องมือสนับสนุนการตัดสินใจ และให้มนุษย์ตรวจสอบอีกครั้งเสมอ

3 การนำ AI ไปใช้ในทางที่ผิด



AI อาจถูกใช้ในทางลบ เช่น การสร้างข่าวปลอม (Fake News) หรือภาพปลอม (Deepfake) ที่อาจส่งผลกระทบต่อสังคมและความเชื่อมั่น

แนวปฏิบัติ: ติดตามข่าวสารเกี่ยวกับภัยจากเทคโนโลยีและใช้เครื่องมือเพื่อตรวจสอบเนื้อหาปลอม

4 ความปลอดภัยของระบบ (Cybersecurity)



AI อาจเป็นเป้าหมายของการโจมตีทางไซเบอร์ เช่น การเจาะระบบเพื่อขโมยข้อมูล หรือการหลอก AI ให้ประมวลผลผิดพลาด (Adversarial Attacks)

แนวปฏิบัติ : เสริมความปลอดภัยของระบบด้วยมาตรการ เช่น การเข้ารหัสและการตรวจสอบความปลอดภัยเป็นประจำ

5 การพึ่งพา AI มากเกินไป



การใช้ AI ในการตัดสินใจที่สำคัญ เช่น ในการแพทย์ หรือการเงิน อาจนำไปสู่ความเสี่ยงหากไม่มีการตรวจสอบอย่างเหมาะสม

แนวปฏิบัติ : ใช้ AI เป็นเครื่องมือเสริม ไม่ใช้การตัดสินใจหลัก และต้องมีแผนสำรองหาก AI ทำงานผิดพลาด

6 ประเด็นด้านจริยธรรม



บางการใช้งานของ AI เช่น หุ่นยนต์สังหารในด้านการทหาร หรือ AI ที่รวบรวมข้อมูลส่วนบุคคลจำนวนมาก อาจก่อให้เกิดคำถามด้านจริยธรรม

แนวปฏิบัติ : ให้ความสำคัญกับหลักจริยธรรมในการพัฒนา AI เช่น การเคารพสิทธิของผู้ใช้และความโปร่งใสในการดำเนินงาน

ข้อคิดสำคัญ: แม้ว่า AI จะช่วยให้ชีวิตสะดวกสบายมากขึ้น แต่การใช้งานอย่างมีสติและเข้าใจในข้อจำกัดของเทคโนโลยี ก็เป็นสิ่งสำคัญไม่แพ้กัน

ผู้จัดทำ กลุ่มดิจิทัลเพื่อส่งเสริมสุขภาพ ศูนย์อนามัยที่ 5 ราชบุรี

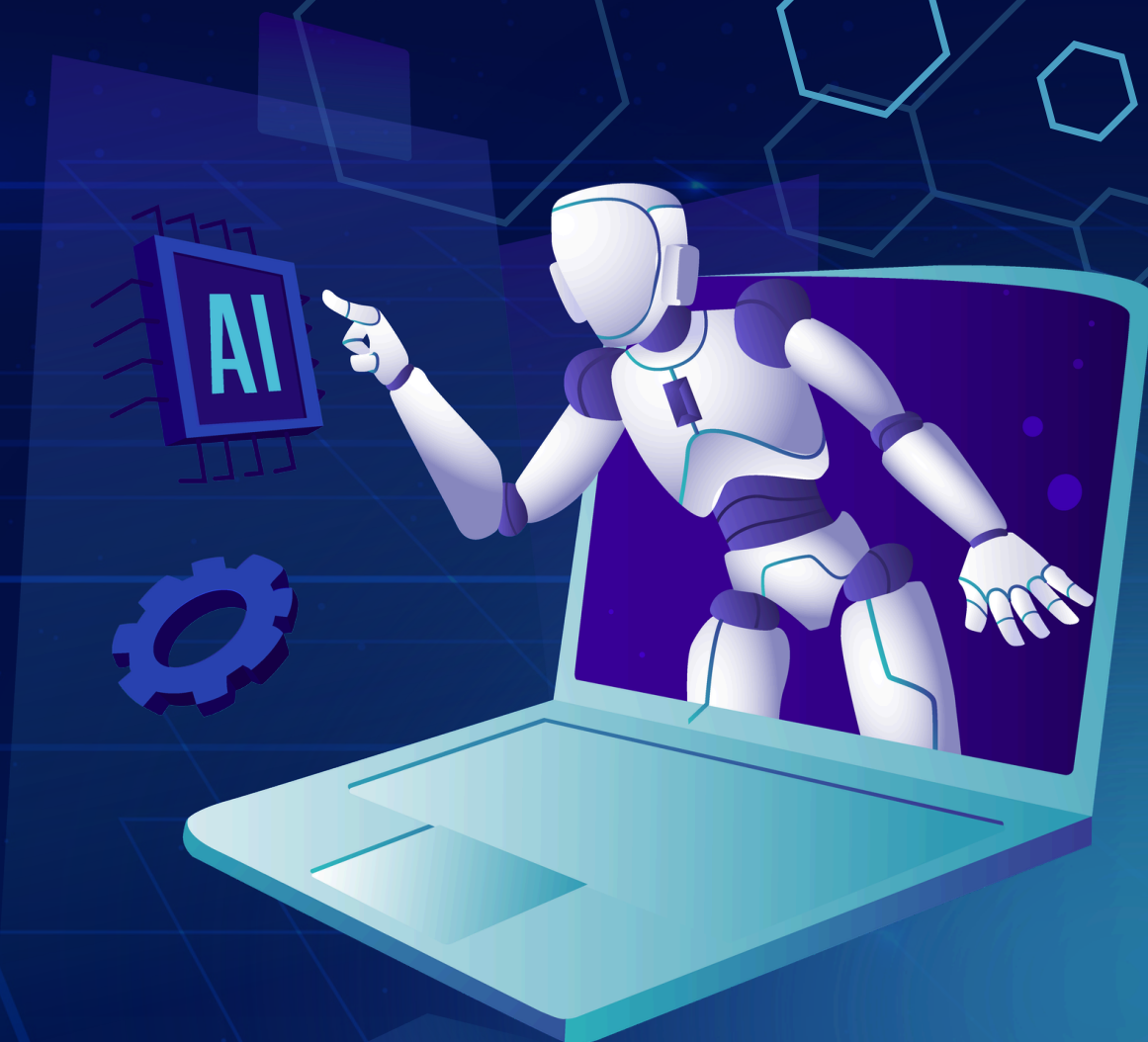
แหล่งข้อมูลอ้างอิง <https://info.apexcircuit.com/?p=30062>

ความเสี่ยงของ AI และแนวทางการใช้งาน อย่างปลอดภัยในยุคดิจิทัล

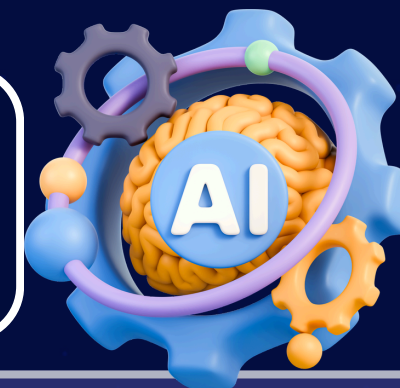
จัดทำโดย

กลุ่มดิจิทัลเพื่อส่งเสริมสุขภาพ

ศูนย์อนามัยที่ 5 ราชบุรี

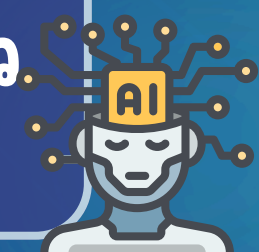


ปัญญาประดิษฐ์ (AI) คืออะไร



ปัญญาประดิษฐ์ (ARTIFICIAL INTELLIGENCE: AI) คือ เทคโนโลยีที่พัฒนาให้ระบบคอมพิวเตอร์และเครื่องจักรมีความฉลาด สามารถคิด วิเคราะห์ เรียนรู้เหตุผล และทำงานเลียนแบบพฤติกรรมมนุษย์ได้ เช่น การประมวลผลภาษา การจดจำภาพ การเรียนรู้ การวางแผน และการแก้ปัญหาต่างๆ

ในยุคที่เทคโนโลยีปัญญาประดิษฐ์ (AI) เติบโตอย่างรวดเร็ว การใช้งาน AI กลายเป็นเรื่องธรรมดา ไม่ว่าจะเป็นหน่วยงานภาครัฐ การสื่อสาร หรือชีวิตประจำวัน แต่ท่ามกลางความสะดวกสบายที่ AI มอบให้ ก็ยังมีความเสี่ยงบางอย่างที่หลายคนอาจไม่ทันได้ระวัง งานดิจิทัลจึงนำความเสี่ยงของ AI ที่ควรรู้ พร้อมแนวทางการใช้งานอย่างปลอดภัย เพื่อให้ใช้ AI ได้อย่างมั่นใจ และไม่ตกเป็นเหยื่อของเทคโนโลยีโดยไม่รู้ตัว



ความเสี่ยงของ AI



1. ความเป็นส่วนตัวและข้อมูลส่วนบุคคล

ปัญหาการละเมิดข้อมูล : AI มักต้องใช้ข้อมูลจำนวนมากในการประมวลผล ซึ่งอาจทำให้ข้อมูลส่วนบุคคลของผู้ใช้รั่วไหลได้



2. ความปลอดภัยและความน่าเชื่อถือของระบบ

ข้อผิดพลาดของ AI : แม้ AI จะมีความแม่นยำ แต่ก็ยังอาจทำผิดพลาดได้ เช่น การวินิจฉัยโรคผิดพลาด หรือข้อเสนอแนะที่ไม่ถูกต้อง



3. การนำ AI ไปใช้ในทางที่ผิด

AI อาจถูกใช้ในทางลบ เช่น การสร้างข่าวปลอม (Fake News) หรือภาพปลอม (Deepfake) ที่อาจส่งผลกระทบต่อสังคมและความเชื่อมั่น



4. ความปลอดภัยของระบบ [CYBERSECURITY]

AI อาจเป็นเป้าหมายของการโจมตีทางไซเบอร์ เช่น การเจาะระบบเพื่อขโมยข้อมูล หรือการหลอก AI ให้ประมวลผลผิดพลาด (Adversarial Attacks)



5. การพึ่งพา AI มากเกินไป

การใช้ AI ในการตัดสินใจที่สำคัญ เช่น ในการแพทย์หรือการเงิน อาจนำไปสู่ความเสี่ยงหากไม่มีการตรวจสอบอย่างเหมาะสม



6. ประเด็นด้านจริยธรรม

บางการใช้งานของ AI เช่น หุ่นยนต์สังหารในด้านการทหาร หรือ AI ที่รวบรวมข้อมูลส่วนบุคคลจำนวนมาก อาจก่อให้เกิดคำถามด้านจริยธรรม

แนวทางการใช้งานอย่างปลอดภัยในยุคดิจิทัล

1. ควรตรวจสอบนโยบายความเป็นส่วนตัวของแพลตฟอร์มที่ใช้ AI และป้องกันข้อมูลส่วนตัว เช่น ชื่อ-นามสกุล, เบอร์โทรศัพท์, อีเมล, วันเกิด, เลขบัตรประชาชน, ที่อยู่ ข้อมูลระบุตัวตนอื่นๆ และไม่ให้สิทธิ์เข้าถึงข้อมูลที่เกิดขึ้นเป็นประจำ

2. ใช้ AI เป็นเพียงเครื่องมือสนับสนุนการตัดสินใจ และให้มนุษย์ตรวจสอบอีกครั้งเสมอ

3. ติดตามข่าวสารเกี่ยวกับภัยจากเทคโนโลยีและใช้เครื่องมือเพื่อตรวจสอบเนื้อหาปลอม

4. เสริมความปลอดภัยของระบบด้วยมาตรการ เช่น การเข้ารหัสและการตรวจสอบความปลอดภัยเป็นประจำ

5. ใช้ AI เป็นเครื่องมือเสริม ไม่ใช่การตัดสินใจหลัก และต้องมีแผนสำรองหาก AI ทำงานผิดพลาด

6. ให้ความสำคัญกับหลักจริยธรรมในการพัฒนา AI เช่น การเคารพสิทธิของผู้ใช้และความโปร่งใสในการดำเนินงาน

แม้ว่า AI จะช่วยให้ชีวิตสะดวกสบายมากขึ้น แต่การใช้งานอย่างมีสติและเข้าใจในข้อจำกัดของเทคโนโลยี ก็เป็นสิ่งสำคัญไม่แพ้กัน

