คอลัมน์ "ร่วมด้วยช่วยคิด" นสพ.ประชาชาติธุรกิจ ฉบับวันที่ 3 – 6 **กรกฎาคม** 2568

AI กับโลกไซเบอร์: เสี่ยงภัย X ปลอดภัย

ดร. นครินทร์ อมเรศ รองผู้อำนวยการ ธนาคารแห่งประเทศไทย

การใช้งานปัญญาประดิษฐ์ **AI** อย่างแพร่หลายในปัจจุบัน ได้อำนวยความสะดวกครอบคลุมตั้งแต่การพัฒนานวัตกรรม การศึกษาวิจัย การดำเนินธุรกิจ จนกระทั่งมาถึงการใช้งานง่าย ๆ ในชีวิตประจำวัน อาทิ การใช้งาน **Generative AI** ยอดนิยม **ChatGPT** หรือ **Gemini** เป็นที่ปรึกษาส่วนตัวที่จะตอบโจทย์ได้ตรงใจตามการปรับแต่ง **Prompt** ของเรา ซึ่งในเมื่อผู้ใช้งานได้ประโยชน์จาก **AI** ขนาดนี้ แล้ว *มิจฉาชีพที่เฝ้าเพียรพยายามคิดมุขใหม่ ๆ มาล่อลวงพวกเราในโลกไซเบอร์จะใช้งาน **AI** ได้ขนาดไหน ?* บทความนี้จึงถอดความและเรียบเรียงประเด็นหารือ[i] ระหว่างตัวจริงเสียงจริงในวงการ คือ ดร.สุพจน์ เธียรวุฒิ และ รศ.ดร. ทศพล ทรรศนพรรณ

เทคโนโลยี AI กับภัยไซเบอร์

อ.สุพจน์ ปูภาพว่า **AI** อยู่กับเราผ่าน **algorithm** ที่อยู่เบื้องหลังประสบการณ์การใช้งานต่าง ๆ โดยเฉพาะ **Generative AI** ที่ถูกใช้งานอย่างหลากหลายในการสร้างสื่อ ซึ่งมิจฉาชีพก็นำมาใช้งาน โดยซุปเปอร์สตาร์คนดังอย่าง **Brad Pitt** ยังถูกสวมรอย ทำให้แม่ม่ายคนหนึ่ง ถูกหลอกจากคนสวมรอยเป็นแม่ของดาราดังว่า ลูกชายอยู่ในโรงพยาบาลและต้องการเงินด่วน ซึ่ง*มิจฉาชีพเองมีความเข้าใจจิตวิทยาเป็นอย่างดี เมื่อเรียนรู้ชีวิตส่วนตัวทาง **social media** ของเราจึงสามารถหลอกได้อย่างแนบเนียน* ซึ่งไม่เพียงแต่เหยื่อจะอยู่ในระดับบุคคล แต่มีกรณีที่บริษัทวิศวกรในสหราชอาณาจักรตกเป็นเหยื่อ **Deepfake scam** กว่า **20** ล้านปอนด์ และมีคดีในลักษณะเดียวกันเกิดขึ้นอย่างต่อเนื่อง

อ.ทศพล รายงานผลที่พบจากการศึกษาสามชิ้นตั้งแต่ **7** ปีก่อน **3** ปีก่อน และที่กำลังศึกษาในปีนี้ พบว่าในอดีตมิจฉาชีพมีการใช้ **Large Language Model (LLM)** ใน **romance scam** โดยมุ่งปรับเปลี่ยนภาษาที่ใช้ในการสื่อสารของมิจฉาชีพให้นุ่มนวลเป็นสุภาพบุรุษ เพื่อหลอกลวงเหยื่อ ทำให้ **AI** ถูกใช้เป็นเครื่องมือในการแปลงสาร แต่ปัจจุบันนี้พบว่า ***AI** สามารถรับ **input** ที่อ้างอิงบริบทของข้อมูลและความสนใจส่วนตัวของเหยื่อ จึงสามารถปรับแต่งเนื้อหาและรูปแบบการสื่อสารให้ตรงจริตของเหยื่อ* และในอนาคตข้างหน้าอาจจะเลยเถิดไปถึงการใช้ **AI** สร้างโลกคู่ขนาน **multiverse** ไปหลอกลวงเหยื่อได้

ขั้นตอนการใช้งาน AI ของมิจฉาชีพ

อ.สุพจน์ ฉายภาพขั้นตอนการใช้งาน **AI** ในการหลอกลวงเหยื่อตามลำดับ คือ **1.** ใช้ข้อมูลจาก **Dark Webs** เพื่อเล็งเป้า **social media** ของเหยื่อ **2.** ติดต่อและสานสัมพันธ์ เพื่อ **build** การมีส่วนร่วมของเหยื่อก่อนที่จะ **3.** ลงมือ **Hook** ให้เหยื่อโอนเงินไปยังบัญชีม้า แล้วตัดการติดต่อเมื่อเหยื่อรู้ตัวเพื่อไม่ให้เจ้าหน้าที่ที่เกี่ยวข้องติดตามได้ ดังนั้น แนวทางป้องกันควรมุ่งไปที่การตัดการติดต่อในขั้นที่ **2.** และ ปิดกั้นการโอนเงินในขั้นตอนที่ **3.**

เทคโนโลยีที่ใช้ในแต่ละขั้นตอนมีความแตกต่างกัน อาทิ **1.** ช่วงเก็บรวบรวมข้อมูล มิจฉาชีพจะวิเคราะห์*พฤติกรรมออนไลน์ของเหยื่อเพื่อหาช่องทางขโมย **Identity*** โดยทำ **Web scraping / data Analytics / phishing email** ดังนั้นแนวทางป้องกัน คือ การปิดกั้นข้อมูลส่วนตัวไม่ให้คนต้องสงสัยเข้าถึงได้ง่าย **2.** ช่วงติดต่อและสานสัมพันธ์ มิจฉาชีพจะ*ปลอมแปลงสถานะทางสังคม* โดยใช้ช่องทางติดต่อที่หลากหลาย ใช้ **Identity Theft / Deepfake** โดยใช้ **Phone call/ SMS / Instant Messaging / Phishing email /chatbot** ดังนั้น เหยื่อต้องป้องกันตัวเองด้วย **Caller ID screening / Digital ID proofing / Deepfake detection /phishing email detection / family secret code** และ **3.** ช่วง **hook** จะใช้ **Payment / Fake web site** ผ่านการชำระเงินออนไลน์ ซึ่งเหยื่อป้องกันได้โดยแจ้งระงับบัญชีเมื่อพบพฤติกรรมต้องสงสัย

พัฒนาการขบวนการมิจฉาชีพ

อ.ทศพล แลกเปลี่ยนผลของการลงพื้นที่สำรวจตามแนวชายแดน ทำให้พบว่าขบวนการมิจฉาชีพข้ามชาติมีจุดเริ่มต้นของเส้นทางการเงินจากเครือข่ายธุรกิจการพนันในเอเชียตะวันออก ต่อมาเมื่อถูกปราบปรามในประเทศต้นทาง จึงแสวงหาพื้นที่ที่เหมาะสมเพื่อมาลงหลักปักฐาน อาทิ ประเทศที่มีความขัดแย้งภายในประเทศเพราะภาครัฐไม่สามารถเข้ามาปราบปรามได้ จึงมีการเคลื่อนย้ายมายังประเทศเพื่อนบ้านของไทย

วิธีการที่มิจฉาชีพจะหาเหยื่อในไทยจะเริ่มจากการเข้าถึงกลุ่มที่เล่นพนันออนไลน์ แล้วทำการ **matching** กับกลุ่มมิจฉาชีพในเครือข่าย โดยในส่วนของไทยเองก็พบว่ามีศูนย์กลางการดำเนินการในพื้นที่ตะวันออก เพราะอยู่ใกล้สนามบินและคนในพื้นที่มีความคุ้นเคยในการทำธุรกิจกับชาวต่างชาติที่นำเงินเข้ามาลงทุนเป็นจำนวนมาก จึงไม่รู้สึกผิดสังเกตในการทำธุรกรรมกับกลุ่มทุนมิจฉาชีพที่ทำธุรกิจบังหน้า ต่างจากในภาคเหนือที่กลุ่มทุนมิจฉาชีพจะต้องเก็บตัวอย่างมิดชิดและนำเงินไปลงทุนในหลักทรัพย์มากกว่าการเปิดธุรกิจโดยตรง ซึ่ง*ผลการศึกษาล่าสุดที่ติดตามประเมินผลจากการปิดชายแดนไทยในช่วงที่ผ่านมา พบว่าเจ้าหน้าที่ในท้องที่ได้รับการร้องเรียนลดลงอย่างชัดเจน แต่มิจฉาชีพอาจเคลื่อนย้ายการปฏิบัติการได้* จึงต้องอาศัยการบังคับใช้กฎหมายเพื่อปราบปรามร่วมกับมาตรการต่าง ๆ อย่างเข้มงวด

ทิศทางและแนวโน้มของมิจฉาชีพ

อ.ทศพล เล่าถึงการศึกษาเมื่อ **7** ปีก่อนที่ทำให้พบว่าการเปลี่ยนแปลงทางสังคมและความก้าวหน้าทางเทคโนโลยีที่นำไปสู่สังคมปัจเจกชน หรือมีการปฏิสัมพันธ์ทางสังคมน้อย ทำให้ความเหงาเป็นเหตุให้เหยื่อถูกหลอกลวงได้ง่าย ขณะที่การศึกษาใน **3** ปีก่อน แสดงให้เห็นว่าคนตกเป็นเหยื่อเพราะแสวงหาโอกาสทางการลงทุนเพื่อสร้างผลตอบแทน และสำหรับการศึกษาในปัจจุบันพบว่าเส้นแบ่งระหว่างเหยื่อและมิจฉาชีพเริ่มบางลงจนทำให้คนที่เผชิญกับปัญหาทางเศรษฐกิจอาจตัดสินใจเข้าร่วมกับมิจฉาชีพได้ ดังนั้นโจทย์วิจัยในอนาคตที่อยากจะทำคือ การติดตามวิธีการสรรหาบุคลากรของขบวนการมิจฉาชีพ ที่น่ากังวลว่า *คนรุ่นใหม่ในยุค **post-modern** ที่ต้องอยู่ในสังคมที่ต้องดิ้นรนเอาตัวรอดแล้ว ค่านิยมด้านศีลธรรมทางสังคมอ่อนแอลง อาจถูกผลักดันให้จำต้องเข้าร่วมองค์กรอาชญากรรมข้ามชาติ โดยเห็นว่าสำคัญกว่าเรื่องคุณธรรม*

อ.สุพจน์ อธิบายแนวโน้มล่าสุดในการใช้ **AI** ใน **social engineering** ผ่าน **Cheapfake** หรือ **Generative AI (LLM, Deepfake)** ที่มีราคาถูกลงและอยู่ในรูปแบบ **platform** สำเร็จรูป, **RPA** จาก **Robotic Process Automation** ที่สามารถ **automate** การทำซ้ำ หรือกระบวนการที่มีกฎเกณฑ์ตายตัว ไปสู่ **Agentic AI** ที่ **automate** การตัดสินใจ การเรียนรู้ และการปรับตัว ตลอดจน มีการใช้ **AIaaS** หรือ **AI-as-a-Service** มาเสริม **Scam-as-a-Service** ซึ่งเป็นแนวทางที่มีตัวกลางในการให้บริการทางเทคโนโลยีให้กับมิจฉาชีพอีกทอดหนึ่ง

มิจฉาชีพจึงสามารถ*ปรับเป้าหมายจาก **random** มาเป็น **segmentation** และเจาะจงมาที่ระดับบุคคลได้ในที่สุด การปลอมแปลงตัวตนจึงเปลี่ยนจากปลอมเป็น **Celeb** มาสู่การเป็นเจ้าหน้าที่ภาครัฐ จนในยุคปัจจุบันที่ปลอมเป็นเพื่อนและครอบครัว และในอนาคตอาจจะเป็น **Faked persons*** ที่ไม่เคยมีตัวตนและไม่สามารถติดตามจับกุมได้อีกเลย

*มาตรการตอบโต้จึงต้องอาศัยความร่วมมือและการแลกเปลี่ยนข้อมูล โดยในการป้องกัน ต้องมี กฎเกณฑ์และ **platform** ในการดำเนินการอย่างเป็นระบบตั้งแต่การตรวจจับและตอบโต้ การรายงานผลการปราบปรามอาชญากรรมและกลไกการจัดการเพื่อควบคุมความเสียหายและเยียวยาผู้เสียหาย รวมถึงการสร้างความตระหนักรู้ในการป้องกันตนเอง ผ่านการรณรงค์อย่างจริงจังและเปิดให้เข้าถึงเครื่องมือในการพัฒนาองค์ความรู้และทักษะทุกช่วงวัย เพื่อให้ประชาชนได้รับองค์ความรู้และมีความพร้อมที่จะรับมือกับมิจฉาชีพได้*

บทความนี้เป็นข้อคิดเห็นส่วนบุคคล ซึ่งไม่จำเป็นต้องสอดคล้องกับข้อคิดเห็นของหน่วยงานที่ผู้เขียนสังกัด

---

[i] การประชุมวิชาการเรื่อง ปัญญาประดิษฐ์: เสี่ยงภัย VS ปลอดภัย จัดโดย ศูนย์ศึกษาปัญหาการพนัน คณะเศรษฐศาสตร์จุฬาลงกรณ์มหาวิทยาลัย ในประเด็น **The Cybercrime ecosystem: Problems and Prospect** โดยมีผู้เข้าร่วมเสวนา คือ ดร.สุพจน์ เธียรวุฒิ กรรมการอิสระและประธานกรรมการเทคโนโลยี ธนาคารไทยพาณิชย์ จำกัด (มหาชน) และ รศ.ดร. ทศพล ทรรศนพรรณ หัวหน้าสำนักวิชานิติศาสตร์ คณะนิติศาสตร์ มหาวิทยาลัยเชียงใหม่ และกรรมการผู้ทรงคุณวุฒิด้านสังคมศาสตร์ คณะกรรมการคุ้มครองข้อมูลส่วนบุคคล