

ประเด็น สังคม ฉบับที่ B50	28 ต.ค. 68	วิทยาลัยการทัพบก
ประเด็น สังคม	สแกมเมอร์กับธุรกิจสีเทา ภัยเงียบที่ท้าทายความมั่นคงของสังคมไทยยุคดิจิทัล	
ประเด็นสำคัญ	- สแกมเมอร์คือใคร และทำไมถึงกลายเป็นปัญหาใหญ่ - ความแตกต่างของ สแกมเมอร์ vs คอลเซ็นเตอร์ - ธุรกิจสีเทา (Gray Economy) กับโลกของ “สแกมเมอร์” ในยุคดิจิทัล - ผลกระทบต่อความมั่นคงของสังคมไทย	



ในยุคที่เทคโนโลยีดิจิทัลเข้ามามีบทบาทในทุกมิติของชีวิตมนุษย์ ความสะดวกสบายในการสื่อสาร การซื้อขาย และการลงทุนผ่านโลกออนไลน์ ได้เปิดประตูให้กับโอกาสทางเศรษฐกิจมากมาย แต่ในขณะเดียวกัน ก็ได้เปิดช่องทางใหม่ให้กับกลุ่มมิจฉาชีพที่แฝงตัวอยู่ในโลกไซเบอร์ หนึ่งในภัยเงียบที่ขยายตัวรวดเร็วและซับซ้อนที่สุด คือ **สแกมเมอร์** หรือกลุ่มผู้หลอกลวงออนไลน์ กลายเป็นหนึ่งในภัยทางสังคมที่เติบโตเร็วที่สุดในศตวรรษนี้ การหลอกลวงผ่านระบบออนไลน์ โทรศัพท์ หรือแอปพลิเคชันต่าง ๆ ไม่เพียงสร้างความเสียหายทางเศรษฐกิจแก่ประชาชนเท่านั้น แต่ยังกระทบต่อความมั่นคงของประเทศในหลายมิติ โดยเฉพาะเมื่อเครือข่ายอาชญากรรมเหล่านี้พัฒนาไปสู่ระดับ “ธุรกิจสีเทา” ที่มีโครงสร้างซับซ้อนและเชื่อมโยงข้ามพรมแดน

"สแกมเมอร์" มีกี่รูปแบบ สแกมเมอร์มีหลายรูปแบบและพัฒนาหลากหลายรูปแบบ อยู่ตลอดเวลา แต่ที่พบบ่อย ได้แก่

โรแมนซ์สแกม (Romance Scam) : หลอกในเชิงความสัมพันธ์ คุญเชิงจิต สร้างโปรไฟล์ปลอมเพื่อให้เหยื่อหลงเชื่อและโอนเงินช่วยเหลือ

ฟิชชิงสแกม (Phishing Scam) : ส่งลิงก์ปลอมผ่านอีเมลหรือข้อความ หลอกให้กรอกข้อมูลส่วนตัวหรือรหัสผ่าน

ลงทุนปลอม (Investment Scam) : ชวนลงทุนที่ให้ผลตอบแทนสูงผิดปกติ เมื่อเหยื่อลงทุนก้อนใหญ่ ก็จะเชิดเงินหนี

ข้อปิ้งปลอม (Online Shopping Scam) : สร้างร้านค้าออนไลน์ปลอมที่เลียนแบบร้านจริง หลอกให้โอนเงินโดยไม่มีสินค้าจริง

คอลเซ็นเตอร์สแกม (Call Center Scam) : โทรหลอกเป็นเจ้าหน้าที่รัฐหรือธนาคาร เพื่อขอข้อมูลหรือให้โอนเงิน
สแกมเมอร์คือใคร และทำไมถึงกลายเป็นปัญหาใหญ่

คำว่า Scammer หมายถึง บุคคลหรือกลุ่มบุคคลที่ใช้กลอุบายหลอกลวงเพื่อให้ได้มาซึ่งทรัพย์สินหรือข้อมูลส่วนตัว โดยอาศัยช่องทางออนไลน์เป็นหลัก เช่น โซเชียลมีเดีย แอปนัดเดท เว็บไซต์ซื้อขาย หรือโทรศัพท์หลวง การหลอกลวงมีหลากหลายรูปแบบ ตั้งแต่ โรแมนซ์สแกม ที่ใช้ความรู้สึกเป็นเครื่องมือ ฟิชซิงสแกม ที่ส่งลิงก์ปลอมเพื่อขโมยข้อมูล ไปจนถึง คอลเซ็นเตอร์สแกม ที่ปลอมตัวเป็นเจ้าหน้าที่รัฐหรือธนาคาร

ในปี 2025 หน่วยงานรัฐรายงานว่า มีผู้เสียหายจากกลโกงออนไลน์มากกว่า 300,000 รายทั่วประเทศ มูลค่าความเสียหายรวมกว่า 50,000 ล้านบาท ซึ่งสะท้อนให้เห็นว่าการหลอกลวงไม่ได้เป็นเพียงอาชญากรรมรายบุคคลอีกต่อไป แต่กลายเป็นระบบธุรกิจที่จัดตั้งอย่างมืออาชีพ



ความแตกต่างของ สแกมเมอร์ vs คอลเซ็นเตอร์

โดยทั่วไป คอลเซ็นเตอร์ คือศูนย์บริการลูกค้าที่ดำเนินการอย่างถูกกฎหมาย มีวัตถุประสงค์เพื่อช่วยเหลือผู้ใช้บริการ รับเรื่องร้องเรียน หรือประชาสัมพันธ์ข้อมูลสินค้าและบริการ ซึ่งพนักงานทุกคนอยู่ภายใต้สัญญาจ้างตามกฎหมายแรงงาน ใช้ระบบโทรศัพท์ที่สามารถตรวจสอบได้จริง และอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคล (PDPA) แต่ แก๊งคอลเซ็นเตอร์ ซึ่งเป็นหนึ่งในรูปแบบของ Scammer กลับใช้โครงสร้างการทำงานที่เหมือนจริงแต่ผิดกฎหมาย มีระบบเวอร์ทำงาน สคริปต์การพูด และสายโทรออกอัตโนมัติ แต่ทั้งหมดมีจุดประสงค์เพื่อหลอกลวงเหยื่อให้โอนเงินหรือเปิดเผยข้อมูลสำคัญ กลุ่มเหล่านี้มักใช้หมายเลขโทรศัพท์ปลอม ซิมชั่วคราว หรือเทคโนโลยี VoIP เพื่อปิดบังต้นทาง และบางส่วนมีฐานปฏิบัติการอยู่ในประเทศเพื่อนบ้าน เช่น เมียนมา กัมพูชา หรือสปป.ลาว

ความแตกต่างระหว่าง คอลเซ็นเตอร์จริง กับ แก๊งคอลเซ็นเตอร์ อยู่ที่ เจตนาและความถูกต้องตามกฎหมาย ฝ่ายแรกให้บริการด้วยความโปร่งใสเพื่ออำนวยความสะดวกแก่ลูกค้า ขณะที่ฝ่ายหลังใช้เทคนิคเดียวกันเพื่อแสวงหาผลประโยชน์โดยมิชอบ ซึ่งเป็นภัยคุกคามต่อเศรษฐกิจและศีลธรรมของสังคม

ธุรกิจสีเทา (Gray Economy) กับโลกของ “สแกมเมอร์” ในยุคดิจิทัล

ในยุคดิจิทัลที่เทคโนโลยีเชื่อมต่อผู้คนทั่วโลกอย่างไร้พรมแดน นอกจากโอกาสทางเศรษฐกิจที่เปิดกว้างขึ้นแล้ว ยังเกิดปรากฏการณ์ทางเศรษฐกิจอีกรูปแบบหนึ่งที่เรียกว่า ธุรกิจสีเทา (Gray Economy) ซึ่งเป็นกิจกรรมทาง

เศรษฐกิจที่อยู่ใน “พื้นที่ก้ำกึ่งระหว่างถูกกฎหมายกับผิดกฎหมาย” และหนึ่งในรูปแบบของธุรกิจสีเทาที่กำลังแพร่ระบาดในสังคมไทยและทั่วโลกในปัจจุบัน คือ “สแกมเมอร์” (Scammer) หรือกลุ่มมิจฉาชีพออนไลน์

สแกมเมอร์เหล่านี้มักอยู่ในเครือข่ายข้ามชาติ มี “ศูนย์ปฏิบัติการ” อยู่ในประเทศเพื่อนบ้าน เช่น เมียนมา ลาว กัมพูชา โดยใช้แรงงานคนไทยและต่างชาติ ซึ่งสะท้อนว่านี่ไม่ใช่อาชญากรรมรายบุคคล แต่คือธุรกิจสีเทาเต็มรูปแบบมีทั้ง นายทุน ผู้จัดการ โปรแกรมเมอร์ คนรับโอนเงิน และทีมหลอกลวงเหยื่อ เหมือนองค์กรธุรกิจทั่วไป ผลกระทบต่อความมั่นคงของสังคมไทย



ศูนย์กลางฟอกเงินดิจิทัล

2. ด้านความมั่นคงและอาชญากรรมข้ามชาติ เครือข่ายสแกมเมอร์จำนวนมากเชื่อมโยงกับกลุ่มค้ายาเสพติดและการใช้แรงงานบังคับ มีการลักลอบตั้งฐานปฏิบัติการในพื้นที่ชายแดน สร้างภาระให้หน่วยงานความมั่นคงต้องระดมทรัพยากรตรวจสอบและปราบปราม

3. ด้านสังคมและศีลธรรม การหลอกลวงออนไลน์ทำให้เกิด สังคมไม่ไว้วางใจกัน ผู้คนเริ่มระแวงต่อการติดต่อทางดิจิทัล ศีลธรรมของเยาวชนบางส่วนถูกบิดเบือน เมื่อเห็นการหลอกลวงเป็น อาชีพทำเงินง่าย

4. การตอบโต้ของรัฐและแนวทางป้องกัน รัฐบาลไทยได้ออกมาตรการหลายด้านในปี 2025 เช่น การออกร่างพระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมออนไลน์ ซึ่งให้อำนาจธนาคาร ผู้ให้บริการโทรศัพท์ และ ดิจิทัล ระบุบัญชีหรือเบอร์ที่เกี่ยวข้องกับการหลอกลวงได้ทันทีโดยไม่ต้องรอคำสั่งศาล รวมถึงการจัดตั้ง ศูนย์ความร่วมมือไทย-กัมพูชา-ลาว เพื่อติดตามเครือข่ายข้ามพรมแดน

ในระดับประชาชน การรู้เท่าทันดิจิทัล (Digital Literacy) เป็นเกราะป้องกันที่สำคัญที่สุด การตรวจสอบข้อมูลก่อนเชื่อ ไม่โอนเงินหรือให้ข้อมูลส่วนตัวกับผู้ที่ไม่รู้จัก รวมถึงการแจ้งเหตุเมื่อพบพฤติกรรมต้องสงสัย คือสิ่งที่ช่วยตัดวงจรอาชญากรรมนี้ได้ดีที่สุด

ผลกระทบต่อความมั่นคงของสังคมไทย

ภัยจากธุรกิจสแกมเมอร์ไม่ได้จำกัดอยู่แค่การสูญเสียทรัพย์สินของประชาชน แต่ยังมีผลกระทบเชิงโครงสร้างในระดับประเทศ ดังนี้

ภัยจากธุรกิจสแกมเมอร์ไม่ได้จำกัดอยู่แค่การสูญเสียทรัพย์สินของประชาชน แต่ยังมีผลกระทบเชิงโครงสร้างในระดับประเทศ ดังนี้

1. ด้านเศรษฐกิจและการเงิน เงินที่ได้จากการหลอกลวงถูกฟอกผ่านระบบธนาคาร e-wallet หรือ คริปโตเคอร์เรนซี ส่งผลให้ระบบการเงินมีความเสี่ยง และบั่นทอนความเชื่อมั่นของนักลงทุนต่างชาติ หากประเทศไทยถูกมองว่าเป็น

1. ด้านเศรษฐกิจและการเงิน เงินที่ได้จากการหลอกลวงถูกฟอกผ่านระบบธนาคาร e-wallet หรือ คริปโตเคอร์เรนซี ส่งผลให้ระบบการเงินมีความเสี่ยง และบั่นทอนความเชื่อมั่นของนักลงทุนต่างชาติ หากประเทศไทยถูกมองว่าเป็น ศูนย์กลางฟอกเงินดิจิทัล

2. ด้านความมั่นคงและอาชญากรรมข้ามชาติ เครือข่ายสแกมเมอร์จำนวนมากเชื่อมโยงกับกลุ่มค้ายาเสพติด และการใช้แรงงานบังคับ มีการลักลอบตั้งฐานปฏิบัติการในพื้นที่ชายแดน สร้างภาระให้หน่วยงานความมั่นคงต้องระดมทรัพยากรตรวจสอบและปราบปราม

3. ด้านสังคมและศีลธรรม การหลอกลวงออนไลน์ทำให้เกิด สังคมไม่ไว้วางใจกัน ผู้คนเริ่มระแวงต่อการติดต่อทางดิจิทัล ศีลธรรมของเยาวชนบางส่วนถูกบิดเบือน เมื่อเห็นการหลอกลวงเป็น อาชีพทำเงินง่าย

4. การตอบโต้ของรัฐและแนวทางป้องกัน รัฐบาลไทยได้ออกมาตรการหลายด้านในปี 2025 เช่น การออกร่างพระราชกำหนดว่าด้วยการป้องกันและปราบปรามอาชญากรรมออนไลน์ ซึ่งให้อำนาจธนาคาร ผู้ให้บริการโทรศัพท์ และ ดิจิทัล ระบุบัญชีหรือเบอร์ที่เกี่ยวข้องกับการหลอกลวงได้ทันทีโดยไม่ต้องรอคำสั่งศาล รวมถึงการจัดตั้ง ศูนย์ความร่วมมือไทย-กัมพูชา-ลาว เพื่อติดตามเครือข่ายข้ามพรมแดน

ในระดับประชาชน การรู้เท่าทันดิจิทัล (Digital Literacy) เป็นเกราะป้องกันที่สำคัญที่สุด การตรวจสอบข้อมูลก่อนเชื่อ ไม่โอนเงินหรือให้ข้อมูลส่วนตัวกับผู้ที่ไม่รู้จัก รวมถึงการแจ้งเหตุเมื่อพบพฤติกรรมต้องสงสัย คือสิ่งที่ช่วยลดวงจรอาชญากรรมนี้ได้ดีที่สุด

ภาครัฐตอบโต้: แนวทางและกฎหมายล่าสุด

ในช่วงปี 2025 รัฐบาลไทยและหน่วยงานที่เกี่ยวข้องมีการผลักดันมาตรการเข้มข้นทั้งด้านกฎหมายและความร่วมมือระหว่างประเทศ เช่น การตั้งคณะทำงานร่วมกับกัมพูชา ประเทศเพื่อนบ้าน เพื่อสกัดการย้ายฐานของแก๊ง การออก/ปรับใช้กฎระเบียบไซเบอร์เพื่อลงโทษผู้เกี่ยวข้อง และมาตรการให้ธนาคาร ผู้ให้บริการมือถือมีบทบาทระบุบัญชีหรือซิมที่ใช้ในกิจกรรมผิดกฎหมายได้รวดเร็วขึ้น (ร่าง พ.ร.ก. และการขยายอำนาจของหน่วยงานที่เกี่ยวข้อง) ทั้งนี้การบังคับใช้ยังต้องการความร่วมมือระหว่างประเทศ เพราะแก๊งมักกระจายตัวข้ามพรมแดน

แนวโน้มของเทคโนโลยี Deepfake และเสียง AI กับการหลอกลวงในอนาคต

เมื่อเทคโนโลยีปัญญาประดิษฐ์ (AI) พัฒนาไปอย่างรวดเร็ว กลุ่มมิจฉาชีพได้เริ่มนำเทคโนโลยี Deepfake และ AI Voice มาใช้สร้างภาพและเสียงปลอมที่สมจริงจนยากจะแยกแยะ ตัวอย่างที่พบในต่างประเทศคือการปลอมเสียงผู้บริหารเพื่อสั่งโอนเงิน หรือสร้างวิดีโอปลอมของบุคคลสำคัญเพื่อบิดเบือนข่าวสาร

แนวโน้มในอนาคตคาดว่าเทคนิคเหล่านี้จะถูกใช้ใน 3 รูปแบบหลัก ได้แก่

1. การปลอมตัวผู้บริหาร (CEO Fraud) เพื่อสั่งการทางการเงิน
2. การหลอกลวงอารมณ์ (Emotional Scam) โดยใช้ภาพหรือเสียงของคนใกล้ชิดขอความช่วยเหลือ
3. การบิดเบือนทางการเมือง (Information Warfare) ที่ใช้ Deepfake สร้างข่าวปลอมเพื่อทำลายความน่าเชื่อถือของสถาบันและผู้นำ

เทคโนโลยีเหล่านี้จึงกลายเป็นภัยคุกคามรูปแบบใหม่ต่อ ความมั่นคงทางดิจิทัล ซึ่งอาจส่งผลกระทบทั้งต่อเศรษฐกิจ การเมือง และจิตวิทยาสังคมในวงกว้าง

แนวทางปฏิบัติสำหรับประชาชน วิธีสังเกตและป้องกันตัว

การมี ความรู้เท่าทันดิจิทัล (Digital Literacy) และ ความฉลาดรู้สื่อ (Media Literacy) เป็นสิ่งจำเป็น ต้องรู้จักตรวจสอบข้อมูลก่อนเชื่อ ไม่โอนเงินให้กับคนที่ไม่รู้จัก และรายงานต่อหน่วยงานรัฐเมื่อพบพฤติกรรมต้อง สงสัย เมื่อได้รับสายแปลก อย่ารีบโอนเงินหรือให้ข้อมูลส่วนตัวเมื่อได้รับการติดต่อแบบเร่งด่วนจากหมายเลขไม่ รู้จัก ให้ตั้งคำถามและยืนยันด้วยช่องทางทางการขององค์กรนั้น ๆ ต้องมีการตรวจสอบ URL และแอปก่อนดาวน์โหลด หลีกเลี่ยงการคลิกลิงก์ที่ส่งมาจากคนไม่รู้จัก นอกจากนี้ต้องไม่รับงานที่ให้เปิดบัญชีหรือรับส่งเงินแทนผู้อื่น หากมีข้อเสนอ งานง่ายได้เงินเร็ว ให้คิดไว้ก่อนว่าเป็นสัญญาณอาจเกี่ยวข้องกับแก๊ง หากสงสัย ให้บันทึกเบอร์ ข้อความ และภาพหน้าจอ และแจ้งความหรือแจ้งหน่วยงานที่เกี่ยวข้อง (ธนาคาร ธปท. ดีอีเอส สำนักงานตำรวจ แห่งชาติ) รายงานช่วยให้หน่วยงานติดตามและระงับบัญชี/ซิมที่ใช้ในการกระทำผิดได้เร็วขึ้น

อนาคตของสังคมไทยท่ามกลางเงามืดของโลกออนไลน์

ธุรกิจสีเทาในยุคปัจจุบันไม่ได้เป็นเพียง “พื้นที่เทา” ทางเศรษฐกิจเท่านั้น แต่เป็น“พื้นที่อันตราย” ที่บั่น ทอนศรัทธา ความมั่นคง และคุณธรรมของสังคม ปรากฏการณ์สแกมเมอร์จึงไม่ใช่เพียงเรื่องของ การ ถูกหลอก แต่ คือภาพสะท้อนของโครงสร้างเศรษฐกิจที่ยังมีจุดอ่อนและช่องโหว่ที่ต้องเร่งแก้ไข ในโลกที่ทุกอย่างออนไลน์ได้ ความรู้เท่าทัน คือเกราะป้องกันที่ดีที่สุดของมนุษย์ยุคใหม่

หากประเทศไทยไม่สามารถสร้างระบบความร่วมมือและการรู้เท่าทันเทคโนโลยีได้ทันต่อการเปลี่ยนแปลง ปรากฏการณ์ สแกมเมอร์ และ Deepfake Scam อาจกลายเป็นวัฒนธรรมแห่งการโกงออนไลน์ที่ฝังรากใน สังคมไทย ซึ่งไม่เพียงบ่อนทำลายเศรษฐกิจ แต่ยังสั่นคลอนศีลธรรม ความไว้วางใจ และความมั่นคงของชาติ เทคโนโลยีสร้างโลกใหม่ได้ แต่หากไร้ศีลธรรม ก็สร้างนรกบนหน้าจอได้เช่นกัน ดังนั้น ในโลกที่ภาพและเสียงอาจ ไม่ใช่ความจริงอีกต่อไป ปัญญา คือเกราะป้องกันเดียวที่แท้จริงของมนุษย์

พ.อ.หญิง ฌักค์ ภักตะภรณ์
อจ. หก. สมย. วทบ.

อ้างอิง

1. <https://www.infoquest.co.th/2025/539829>
2. <https://thestandard.co/key-messages-call-center-gangs>
3. <https://www.naewna.com/inter/923123>
4. <https://www.dailynews.co.th/news/5234928>
5. <https://thaipublica.org/2025/01/cabinet-approves-law-to-crack-down-on-call-centers>
6. <https://policywatch.thaipbs.or.th/article/government-124>