



Scammer

ภัยร้ายใกล้ตัวในชีวิตดิจิทัลของคนไทย

Scammer ภัยร้ายใกล้ตัวในชีวิตดิจิทัลของคนไทย

KEY SUMMARY

ภัยสแกมเมอร์ในไทยยังเป็นประเด็นที่น่ากังวล และในปีนี้จะสร้างความเสียหายแล้วไม่ต่ำกว่า 9.3 พันล้านบาท โดยการหลอกลวงผ่านการซื้อสินค้าและบริการออนไลน์เป็นเคสที่ได้รับแจ้งเหตุสูงสุด

โดยในช่วงเดือนมกราคม – กรกฎาคมที่ผ่านมา ศูนย์ต่อต้านการฉ้อโกงออนไลน์ได้รับแจ้งเหตุอาชญากรรมทางเทคโนโลยีหรือเหตุจากภัยสแกมเมอร์แล้วกว่า 1.9 แสนเคส มูลค่าความเสียหายรวมกว่า 9.3 พันล้านบาท ซึ่งแม้แนวโน้มจำนวนการรับแจ้งเหตุจะลดลงมาอยู่ที่เฉลี่ย 902 เคสต่อวันในปีนี้อย่างเทียบเท่ากับปี 2025 ที่ราว 1,040 เคสต่อวัน แต่จำนวนการรับแจ้งเหตุถือว่ายังอยู่ในระดับสูง โดยเฉพาะการหลอกลวงผ่านการซื้อสินค้าและบริการออนไลน์ที่ได้รับแจ้งเหตุสูงสุดที่ 1.39 แสนเคสหรือประมาณ 73% ของจำนวนรับแจ้งเหตุทั้งหมด นอกจากนี้การที่โซเชียลมีเดียเข้ามามีบทบาทสำคัญในชีวิตประจำวันของคนยุคใหม่ จึงทำให้แพลตฟอร์มเหล่านี้กลายเป็นช่องทางหลักที่สแกมเมอร์ใช้เข้าถึงเป้าหมาย และส่งผลให้ผู้ใช้งานเผชิญความเสี่ยงในการตกเป็นเหยื่อเพิ่มขึ้น

คนไทยยังเผชิญความเสี่ยงจากภัยสแกมเมอร์อย่างต่อเนื่อง จากผลสำรวจของ SCB EIC พบว่าราว 1 ใน 4 ของผู้ตอบแบบสอบถามเคยตกเป็นเหยื่อและได้รับความเสียหาย ซึ่งส่วนใหญ่เกิดจากการซื้อสินค้าและบริการออนไลน์

ในมุมมองผู้บริโภคจากผลสำรวจ SCB EIC Consumer survey “When Life Goes Digital : เทคโนโลยีดิจิทัลมีผลต่อชีวิตคุณอย่างไร?” พบว่า ทุกวันนี้คนไทยยังเผชิญกับความพยายามหลอกลวงจากสแกมเมอร์ แต่ที่น่ากังวลคือราว 1 ใน 4 ของผู้ตอบแบบสอบถามเคยได้รับความเสียหายจากสแกมเมอร์มาแล้ว โดยรูปแบบที่พบบ่อยที่สุดคือการหลอกลวงให้ซื้อสินค้าและบริการออนไลน์ ทั้งนี้ผู้ได้รับความเสียหายมากกว่าครึ่งยังระบุว่าความเสียหายที่เกิดขึ้นส่วนใหญ่ไม่ได้รับการแก้ไขหรือเยียวยาทั้งในกรณีซื้อสินค้าและบริการแล้วไม่ได้รับสินค้า และการถูกหลอกลวงโอนเงินจากแก๊งคอลเซ็นเตอร์ ในทางกลับกัน ความเสียหายจากกรณีการถูกดัดบัตรเครดิตโดยไม่ได้รับอนุญาตมีแนวโน้มได้รับการแก้ไขค่อนข้างสูง สะท้อนถึงกลไกของสถาบันการเงินที่สามารถตรวจสอบและระงับธุรกรรมที่ผิดปกติได้อย่างทัน่วงที

ความกังวลต่อภัยสแกมเมอร์ส่งผลให้คนไทยหันไปเลือกซื้อสินค้าและบริการออนไลน์บนแพลตฟอร์มรายใหญ่หรือช่องทางของแบรนด์ทางการมากขึ้น ขณะที่ร้านค้าขนาดเล็ก-กลางยังสามารถสร้างความเชื่อมั่นจากผู้บริโภคได้ หากแสดงข้อมูลที่ชัดเจนและได้รับการรับรองจากแพลตฟอร์ม

ปัจจุบันการซื้อสินค้าและบริการผ่านช่องทางออนไลน์ได้กลายเป็นส่วนหนึ่งของวิถีชีวิตของคนไทยในยุคดิจิทัล แม้จะยังมีความเสี่ยงจากภัยสแกมเมอร์ก็ตาม โดยผู้บริโภคยังคงเชื่อมั่นว่าการซื้อสินค้าและบริการออนไลน์ผ่านแพลตฟอร์ม e-Commerce รายใหญ่และแพลตฟอร์มทางการของแบรนด์โดยตรงมีความปลอดภัยมากกว่า อย่างไรก็ตาม หลายคนยังเลือกหลีกเลี่ยงการผูกบัตรเครดิตหรือบัญชีธนาคารกับแพลตฟอร์มเพื่อลดความเสี่ยงจากการถูกเข้าถึงข้อมูลทางการเงินโดยไม่ได้รับอนุญาต ขณะที่การซื้อสินค้าและบริการออนไลน์กับร้านค้าขนาดเล็ก-

กลาง ผู้บริโภคจะให้ความสำคัญกับความน่าเชื่อถือของร้านค้าเป็นหลัก โดยมักพิจารณาข้อมูลร้านค้า ประวัติการดำเนินงาน และรีวิวจากผู้ใช้งานรายอื่นก่อนตัดสินใจ ดังนั้น ร้านค้าควรให้ข้อมูลและช่องทางการติดต่อที่ครบถ้วน ชัดเจน และตรวจสอบได้ ในขณะเดียวกัน สันติลักษณ์รับรองร้านค้าที่ออกโดยแพลตฟอร์มจะช่วยยืนยันความน่าเชื่อถือให้กับผู้บริโภคได้ในระดับหนึ่ง

ธุรกิจ e-Commerce และร้านค้าออนไลน์จำเป็นต้องยกระดับด้านความปลอดภัยอย่างต่อเนื่องเพื่อเสริมสร้างความเชื่อมั่นและความไว้วางใจให้แก่ผู้บริโภค

ปัจจุบัน ผู้ให้บริการแพลตฟอร์ม e-Commerce ต่างยกระดับมาตรฐานความปลอดภัยและสร้างกลไกคุ้มครองผู้บริโภคอย่างต่อเนื่องทั้งการใช้เทคโนโลยี AI ในการตรวจจับสแกนเมอร์ที่แฝงตัวเข้ามา การคัดกรองร้านค้าอย่างเข้มงวด ตลอดจนการสร้างกลไกคุ้มครองผู้บริโภคอย่างการชะลอการจ่ายเงินให้ร้านค้าจนกว่าผู้ซื้อจะยืนยันการได้รับสินค้า ขณะเดียวกัน ร้านค้าที่ต้องการขยายช่องทางการขายสู่ตลาดออนไลน์ก็ควรให้ความสำคัญกับการสร้างความเชื่อมั่นด้านความปลอดภัยแก่ผู้บริโภคด้วยเช่นกัน ไม่ว่าจะเป็น 1. **การให้ข้อมูลอย่างครบถ้วนและตรวจสอบได้** ครอบคลุมทั้งข้อมูลร้านค้า รายละเอียดสินค้า เงื่อนไขการสั่งซื้อ การรับประกันสินค้า ตลอดจนการแสดงผลรีวิวจากผู้ใช้จริง รวมถึงระบบบริการลูกค้าที่สามารถแก้ไขปัญหาได้อย่างทันท่วงทีและมีประสิทธิภาพ 2. **การกำหนดนโยบายคุ้มครองผู้บริโภคที่โปร่งใสและเป็นธรรม** เช่น เงื่อนไขการรับประกันความพึงพอใจในสินค้าและบริการ การคืนเงิน/เปลี่ยนสินค้า/การชดเชยเมื่อสินค้าเกิดปัญหา และ 3. **การนำเทคโนโลยีด้านความปลอดภัยมาใช้** เช่น ระบบรักษาความปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคลเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต รวมถึงการเลือกใช้บริการชำระเงินที่ได้รับการรับรองมาตรฐานสากลเพื่อสร้างความมั่นใจให้แก่ผู้บริโภคในทุกขั้นตอนการซื้อสินค้า

ในขณะเดียวกัน ภาครัฐอาจพิจารณายกระดับมาตรการป้องกันและปราบปรามภัยสแกนเมอร์ ผ่านการออกกฎหมายให้ครอบคลุมยิ่งขึ้น การบูรณาการข้อมูลและความร่วมมือระหว่างหน่วยงาน ตลอดจนการนำเทคโนโลยีขั้นสูงมาใช้ในการตรวจจับและแจ้งเตือนภัย

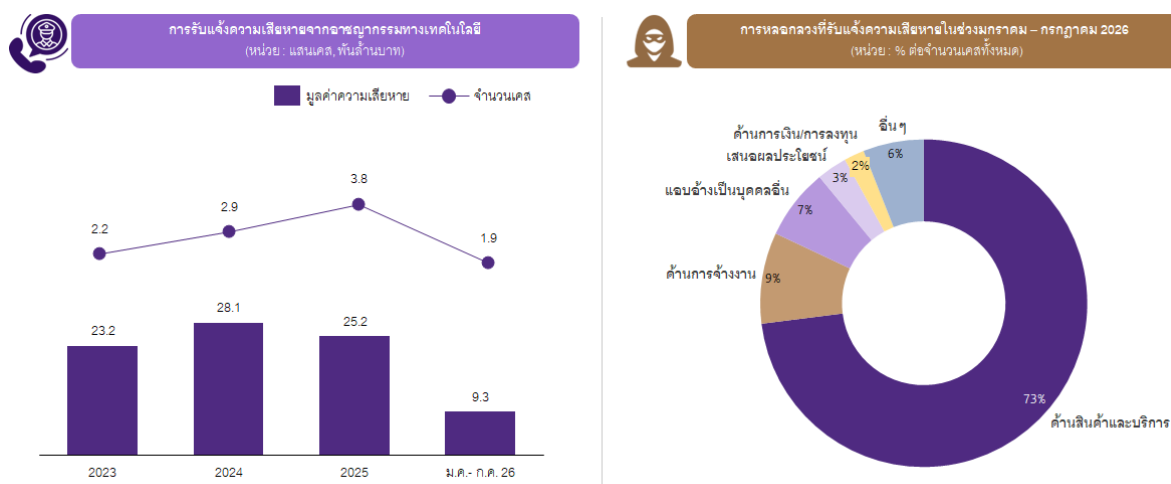
การปราบปรามสแกนเมอร์ถือเป็น “วาระแห่งชาติ” ที่ภาครัฐได้ออกมาตรการเชิงรุกหลายด้าน อาทิ การสกัดกั้นเครือข่ายสแกนเมอร์ตามแนวชายแดน การยกระดับความร่วมมือระหว่างประเทศ การอายัดบัญชีที่เกี่ยวข้อง รวมถึงการนำเทคโนโลยีมาใช้วิเคราะห์ข้อมูลสแกนเมอร์ อย่างไรก็ตาม ภาครัฐอาจพิจารณาการเพิ่มเติมเพื่อเพิ่มประสิทธิภาพในการป้องกันและปราบปรามสแกนเมอร์ อย่างเช่น 1. **การออกกฎหมายที่เข้มงวดและครอบคลุมมากขึ้น** ด้วยการขยายกรอบกฎหมายเพิ่มความรับผิดชอบให้แก่ภาคธุรกิจที่เกี่ยวข้องผ่านการกำหนดบทลงโทษที่ชัดเจนในกรณีที่ไม่ปฏิบัติตามการป้องกันการฉ้อโกง หรือระบบรักษาความปลอดภัยไม่มีประสิทธิภาพเพียงพอจนเปิดช่องให้สแกนเมอร์สร้างความเสียหายแก่ผู้บริโภค 2. **การยกระดับการบูรณาการข้อมูลและความร่วมมือระหว่างหน่วยงาน** ผ่านการจัดตั้งคณะทำงานร่วมระหว่างเจ้าหน้าที่ภาครัฐ สถาบันการเงิน และผู้ให้บริการแพลตฟอร์มดิจิทัล เพื่อเสริมประสิทธิภาพในการรับมือปัญหาสแกนเมอร์ รวมทั้งเพิ่มความสามารถในการตรวจจับและระงับภัยคุกคามได้อย่างทันท่วงทีแบบเรียลไทม์ และ 3. **การประยุกต์ใช้เทคโนโลยีสมัยใหม่ในการป้องกันและแจ้งเตือนภัย** อย่างการนำเทคโนโลยี AI และการวิเคราะห์ข้อมูลมาใช้ในการพัฒนาเครื่องมือป้องกันภัยให้แก่ประชาชน เช่น ระบบหรือแอปพลิเคชันแจ้งเตือนภัยสแกนเมอร์ระดับชาติที่จะช่วยลดโอกาสที่ประชาชนจะตกเป็นเหยื่อของการฉ้อโกงจากเหล่าสแกนเมอร์ได้

ความก้าวหน้าของเทคโนโลยีดิจิทัลได้กลายเป็นส่วนหนึ่งในชีวิตประจำวันของคนไทย ทำให้วิถีการดำเนินชีวิต สะดวกสบายและรวดเร็วมากยิ่งขึ้น ไม่ว่าจะเป็นการติดต่อสื่อสาร การเข้าถึงข้อมูลข่าวสาร หรือการทำธุรกรรมทางการเงิน อย่างไรก็ตาม การพัฒนาอย่างรวดเร็วของเทคโนโลยีนี้ได้เปิดช่องให้เหล่าสแกมเมอร์นำไปใช้เป็นเครื่องมือในการก่อ ก่อโกงในรูปแบบที่ซับซ้อนและแนบเนียนมากขึ้น ส่งผลให้อาชญากรรมทางเทคโนโลยีกลายเป็นภัยใกล้ตัวที่มีโอกาส เกิดขึ้นได้กับทุกคนผ่านหลายช่องทางทั้งโทรศัพท์ ข้อความ หรือโซเชียลมีเดีย ซึ่งก่อให้เกิดความเสี่ยงต่อการสูญเสีย ทรัพย์สินและการรั่วไหลของข้อมูลส่วนบุคคล

สแกมเมอร์ : ภัยเงียบที่ยังสร้างความเสียหายต่อเนื่อง

อาชญากรรมทางเทคโนโลยีหรือภัยสแกมเมอร์ในไทยยังคงเป็นประเด็นที่น่ากังวล จากจำนวนการถูก หลอกหลวงโดยสแกมเมอร์ที่ยังอยู่ในระดับสูง โดยในช่วงเดือนมกราคม - กรกฎาคมที่ผ่านมา ศูนย์ต่อต้านการ ฉ้อโกงออนไลน์ (Anti Cyber Scam Center) สำนักงานตำรวจแห่งชาติ ได้รับแจ้งเหตุอาชญากรรมทางเทคโนโลยีแล้ว มากกว่า 1.9 แสนเคส มูลค่าความเสียหายรวมสูงถึง 9.35 พันล้านบาท ซึ่งแม้แนวโน้มจำนวนการรับแจ้งเหตุจะลดลง จากปี 2025 ที่เฉลี่ยราว 1,040 เคสต่อวันมาอยู่ที่ 902 เคสต่อวัน แต่ถือว่าจำนวนการรับแจ้งเหตุเฉลี่ยยังอยู่ในระดับสูง แม้ภาครัฐจะเร่งปราบปรามอย่างจริงจังและดำเนินการอย่างต่อเนื่อง รวมถึงประชาชนเริ่มรู้เท่าทันกลโกงของเหล่า สแกมเมอร์มากขึ้น แต่ระดับความเสียหายจากอาชญากรรมทางเทคโนโลยียังคงอยู่ในระดับสูง อีกทั้ง สแกมเมอร์ยัง ปรับเปลี่ยนกลวิธีและรูปแบบการหลอกหลวงให้แนบเนียนและซับซ้อนมากขึ้นซึ่งยากต่อการปราบปรามให้ทันทั่วถึง

รูปที่ 1 : อาชญากรรมทางเทคโนโลยีที่ได้รับแจ้งความเสียหาย



หมายเหตุ : ข้อมูลในปี 2023-2025 ประเมินจากข้อมูลสถิติที่เผยแพร่ตามสื่อ
ที่มา : การวิเคราะห์โดย SCB EIC จากข้อมูลของศูนย์ต่อต้านการฉ้อโกงออนไลน์

ปัจจุบันปัญหาการหลอกหลวงผ่านการซื้อสินค้าและบริการออนไลน์ยังคงน่ากังวล จากสถิติการรับแจ้ง เหตุการหลอกหลวงของศูนย์ต่อต้านการฉ้อโกงออนไลน์ พบว่า ในช่วง 7 เดือนที่ผ่านมา การหลอกหลวงผ่านการซื้อสินค้า และบริการเป็นรูปแบบการหลอกหลวงที่มีจำนวนการรับแจ้งเหตุสูงสุดถึง 1.39 แสนเคสหรือคิดเป็นประมาณ 73% ของจำนวนที่ได้รับแจ้งทั้งหมด ตามด้วยการหลอกหลวงเพื่อการจ้างงานหรือหารายได้พิเศษ 1.7 หมื่นเคส (10%)

และการหลอกลวงด้วยการแอบอ้างเป็นบุคคลอื่น/เจ้าหน้าที่ 1.2 หมื่นเคส (6%) โดยทั้ง 3 รูปแบบรวมกันคิดเป็นสัดส่วนสูงถึง 90% และล้วนเป็นกับดักการหลอกลวงที่สแกมเมอร์ใช้กลไกทางจิตวิทยาให้ผู้เสียหายโอนเงินหรือส่งมอบทรัพย์สินด้วยความสมัครใจ ขณะที่กรณีฟิชซิงและโจมตีทางเทคนิคจากการถูกเจาะระบบหรือขโมยข้อมูลมีสัดส่วนการรับแจ้งเหตุต่ำกว่า 1% และจำนวนการรับแจ้งเหตุลดลงอย่างเห็นได้ชัด สะท้อนถึงระบบป้องกันภัยคุกคามทางไซเบอร์ในปัจจุบันที่มีความเข้มแข็งและมีประสิทธิภาพมากขึ้น

โซเชียลมีเดียได้กลายเป็นเครื่องมือหลักที่เหล่าสแกมเมอร์ใช้ในการเข้าถึงเป้าหมาย หากพิจารณาช่องทางการถูกหลอกลวง พบว่า ทางศูนย์ฯ ได้รับแจ้งการถูกหลอกลวงผ่านโซเชียลมีเดีย (เช่น Facebook, TikTok, Instagram, Line) ในสัดส่วนสูงถึง 72% เนื่องจากเป็นช่องทางที่สามารถเข้าถึงผู้คนได้ง่าย รวดเร็ว และเป็นส่วนหนึ่งของการใช้งานในชีวิตประจำวัน จึงทำให้ผู้ใช้งานโซเชียลมีเดียมีโอกาสตกเป็นเป้าหมายของสแกมเมอร์ได้ง่าย รองลงมาคือการหลอกลวงผ่านทางโทรศัพท์ในรูปแบบแก๊งคอลเซ็นเตอร์ (4%) นอกจากนี้ ยังพบการรับแจ้งการหลอกลวงในช่องทางอื่นๆ เช่น แอปพลิเคชันหาคู่ อีเมล และเว็บไซต์ต่าง ๆ สะท้อนถึงการปรับกลวิธีการหลอกลวงของสแกมเมอร์ให้สอดคล้องกับพฤติกรรมการใช้งานเทคโนโลยีดิจิทัลของผู้คนในปัจจุบัน ซึ่งแม้โซเชียลมีเดียจะช่วยเพิ่มความสะดวกสบายในการดำเนินชีวิต แต่ขณะเดียวกันก็แฝงมาด้วยความเสี่ยงและภัยคุกคามที่ผู้ใช้งานจำเป็นต้องตระหนักและใช้งานด้วยความระมัดระวังมากยิ่งขึ้น

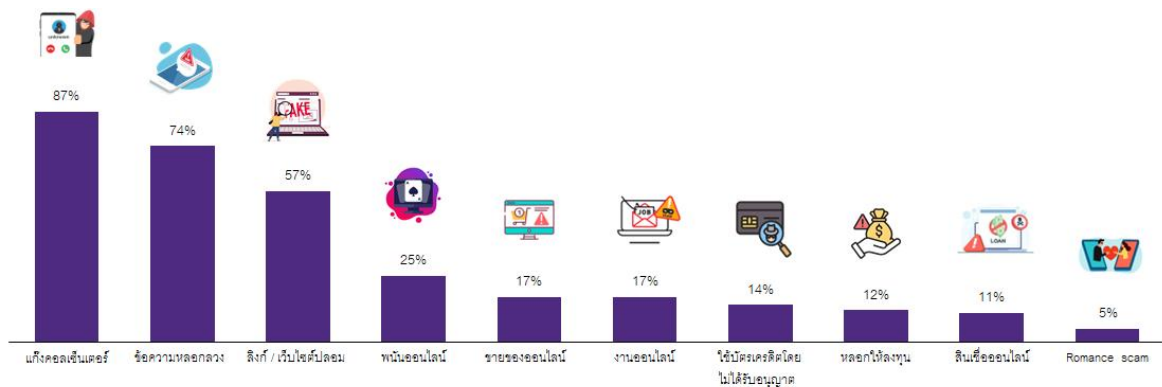
คนไทยยังเผชิญกับความเสี่ยงจากภัยคุกคามจากสแกมเมอร์

ขณะเดียวกัน มุมมองของคนไทยต่อภัยคุกคามจากสแกมเมอร์ในหลายประเด็นสอดคล้องกับสถิติการหลอกลวงที่ได้รับแจ้งเหตุข้างต้น โดยมุมมองส่วนใหญ่ถูกสะท้อนผ่านผลสำรวจ SCB EIC Consumer survey “When Life Goes Digital : เทคโนโลยีดิจิทัลมีผลต่อชีวิตคุณอย่างไร?” ซึ่งพบประเด็นสำคัญ ดังนี้

ในปีที่ผ่านมา คนไทยยังเผชิญกับการพยายามหลอกลวงของสแกมเมอร์โดยเฉพาะจากแก๊งคอลเซ็นเตอร์และการส่งข้อความ โดยผู้ตอบแบบสอบถามถึง 87% เคยได้รับสายโทรศัพท์จากแก๊งคอลเซ็นเตอร์ที่มักจะแอบอ้างเป็นบุคคลหรือเจ้าหน้าที่จากหน่วยงานต่าง ๆ เพื่อหลอกให้โอนเงิน ขณะที่ 75% เคยได้รับข้อความหลอกลวงผ่าน SMS สอดคล้องกับข้อมูลสถิติของ Whoscall ซึ่งเป็นแอปพลิเคชันระบุตัวตนสายโทรเข้าและบล็อกสแปมชั้นนำ พบว่า ในปี 2025 คนไทยตกเป็นเป้าหมายของแก๊งคอลเซ็นเตอร์สูงถึง 39 ล้านครั้งเพิ่มขึ้นจากปี 2024 ราว 1 ล้านครั้ง และ SMS หลอกลวงกว่าอีก 134 ล้านข้อความเพิ่มขึ้นจากปี 2024 กว่า 4 ล้านข้อความ ซึ่งปัจจุบันภาครัฐได้เร่งดำเนินการกวาดล้างแก๊งคอลเซ็นเตอร์แบบบูรณาการทั้งการเข้ามาตราทางกฎหมายผ่านพระราชกำหนด (พ.ร.ก.) มาตราการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี การทำงานร่วมกับสำนักงานกสทช. ตัดวงจรโทรคมนาคมและอินเทอร์เน็ตชายแดนที่คาดว่าเป็นพื้นที่ฐานปฏิบัติการของแก๊งคอลเซ็นเตอร์ และการร่วมมือระหว่างประเทศเพื่อหลายต้นตอของขบวนการ ส่งผลให้การแจ้งเหตุการหลอกลวงในรูปแบบนี้ทยอยลดลงอย่างต่อเนื่อง

รูปที่ 2 : ภัยคุกคามสแกมเมอร์ที่คนไทยเผชิญในปีที่ผ่านมา

หน่วย : % ของผู้ตอบแบบสอบถามทั้งหมด

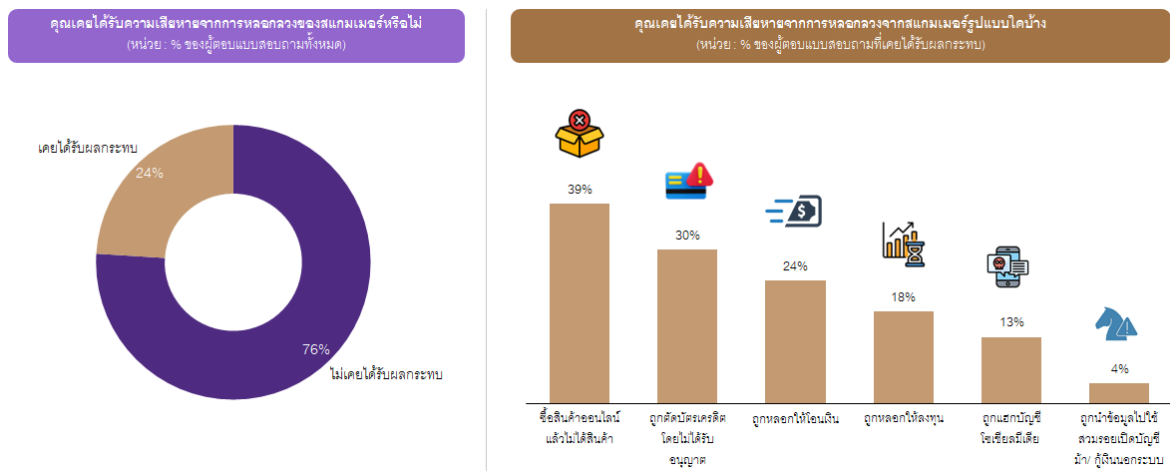


คำถาม : ในช่วง 6 เดือนที่ผ่านมา คุณเคยได้รับการติดต่อที่สงสัยว่าจะเป็นกลลวงทางดิจิทัล (Scam) ในรูปแบบใดบ้าง? (ตอบได้มากกว่า 1 ข้อ)

ที่มา : การวิเคราะห์โดย SCB EIC จากข้อมูลของผลสำรวจความคิดเห็นผู้บริโภค "When Life Goes Digital : เทคโนโลยีดิจิทัลมีผลต่อชีวิตคุณอย่างไร" ในช่วงวันที่ 20 พฤศจิกายน - 11 ธันวาคม 2025

คนไทยราว 1 ใน 4 เคยตกเป็นเหยื่อและได้รับความเสียหายจากการหลอกลวงของสแกมเมอร์ โดยส่วนใหญ่มาจากการหลอกลวงผ่านการซื้อสินค้าและบริการออนไลน์ ผลสำรวจความคิดเห็นผู้บริโภคของ SCB EIC ยังชี้ให้เห็นว่า ราว 24% ของผู้ตอบแบบสอบถามทั้งหมด เคยได้รับความเสียหายจากการถูกหลอกลวง ซึ่งแม้คนไทยจะถูกก่อวินโดยแก๊งคอลเซ็นเตอร์และข้อความหลอกลวงในระดับความถี่ที่ค่อนข้างสูง หากพิจารณาเฉพาะกลุ่มผู้ได้รับผลกระทบโดยตรง พบว่า ความเสียหายที่เกิดจากการซื้อสินค้าและบริการออนไลน์แล้วไม่ได้รับสินค้ามีสัดส่วนสูงถึง 39% สอดคล้องกับข้อมูลการรับแจ้งเหตุของศูนย์ต่อต้านการฉ้อโกงออนไลน์ที่ระบุว่า การหลอกลวงจากการซื้อสินค้าและบริการเป็นรูปแบบความเสียหายที่ได้รับแจ้งเหตุสูงสุด ทั้งนี้ยังพบว่ากลุ่มที่เผชิญความเสียหายในกรณีดังกล่าวส่วนใหญ่เป็นกลุ่มอายุ 46 ปีขึ้นไป (Gen X และ Baby boomer) สะท้อนว่าผู้สูงอายุอาจเป็นกลุ่มเปราะบางที่ตกเป็นเป้าหมายของสแกมเมอร์ได้ง่ายกว่า ซึ่งโดยมากจะเป็นกลุ่มที่กำลังซื้อสูงที่มีการใช้จ่ายผ่านช่องทางออนไลน์เพิ่มขึ้นต่อเนื่อง และหลายกรณีอาจขาดความระมัดระวังในการตรวจสอบข้อมูลความน่าเชื่อถือของผู้ขายอย่างเพียงพอ นอกจากนี้ ยังพบความเสียหายจากการถูกตัดบัตรเครดิตโดยไม่ได้รับอนุญาตในสัดส่วน 30% ซึ่งส่วนหนึ่งเกิดจากการถูกกลุ่มสแกมเมอร์เข้ามาแสกข้อมูลจากร้านค้าหรือเว็บไซต์ที่เคยผูกบัตรเครดิตไว้ หรือการทำบัตรเครดิตสูญหายแล้วผู้อื่นนำไปใช้

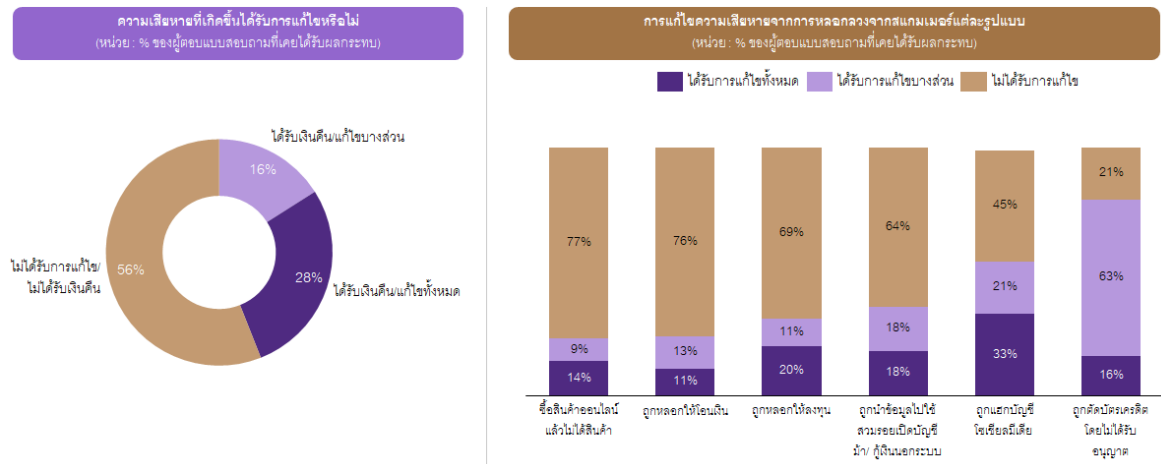
รูปที่ 3 : ความเสียหายจากการหลอกลวงของสแกมเมอร์



ที่มา : การวิเคราะห์โดย SCB EIC จากข้อมูลของผลสำรวจความคิดเห็นผู้บริโภค “When Life Goes Digital : เทคโนโลยีดิจิทัลมีผลต่อชีวิตคุณอย่างไร?” ในช่วงวันที่ 20 พฤศจิกายน – 11 ธันวาคม 2025

แม้ว่าความเสียหายจากการถูกหลอกลวงผ่านการซื้อสินค้าและบริการส่วนใหญ่จะไม่ได้รับการแก้ไขหรือเยียวยา แต่คนไทยยังมีความเชื่อมั่นต่อการซื้อสินค้าและบริการทางออนไลน์ค่อนข้างสูง โดยผู้ได้รับความเสียหายกว่า 56% ระบุว่าความเสียหายที่เกิดขึ้นจากการถูกหลอกลวงจากสแกมเมอร์ไม่ได้รับการแก้ไขเยียวยาหรือไม่ได้รับเงินคืนจากเหตุที่เกิดขึ้น โดยกรณีที่ไม่ได้รับการแก้ไขส่วนใหญ่เป็นการซื้อสินค้าและบริการแล้วไม่ได้รับสินค้า ซึ่งมีสัดส่วนสูงถึง 77% ใกล้เคียงกับกรณีการถูกหลอกให้โอนเงินจากแก๊งคอลเซ็นเตอร์ (76%) ตามด้วยการถูกหลอกให้ลงทุน (69%) ในทางกลับกัน ความเสียหายจากการถูกตัดบัตรเครดิตโดยไม่ได้รับอนุญาตเป็นกรณีที่มีแนวโน้มได้รับการแก้ไขทั้งหมดหรือแก้ไขบางส่วนในสัดส่วนค่อนข้างสูง (79%) ซึ่งสะท้อนถึงกลไกของสถาบันการเงินที่สามารถตรวจสอบและระงับธุรกรรมที่ผิดปกติได้อย่างทันท่วงที อย่างไรก็ตาม แม้ความเสียหายจากการถูกหลอกลวงผ่านการซื้อสินค้าและบริการออนไลน์ยังอยู่ในระดับสูงและส่วนใหญ่ไม่ได้รับการแก้ไข แต่ผู้บริโภคถึง 49% ยังคงเชื่อว่าการซื้อสินค้าและบริการผ่านช่องทางออนไลน์มีความปลอดภัย ขณะที่เพียง 13% มองว่าไม่ปลอดภัยซึ่งส่วนใหญ่เป็นกลุ่มผู้สูงอายุวัยเกษียณที่ยังมีความกังวลต่อความเสี่ยงในการทำธุรกรรมผ่านระบบออนไลน์อยู่

รูปที่ 4 : การแก้ไขหรือเยียวยาจากความเสียหายที่เกิดขึ้นจากสแกมเมอร์

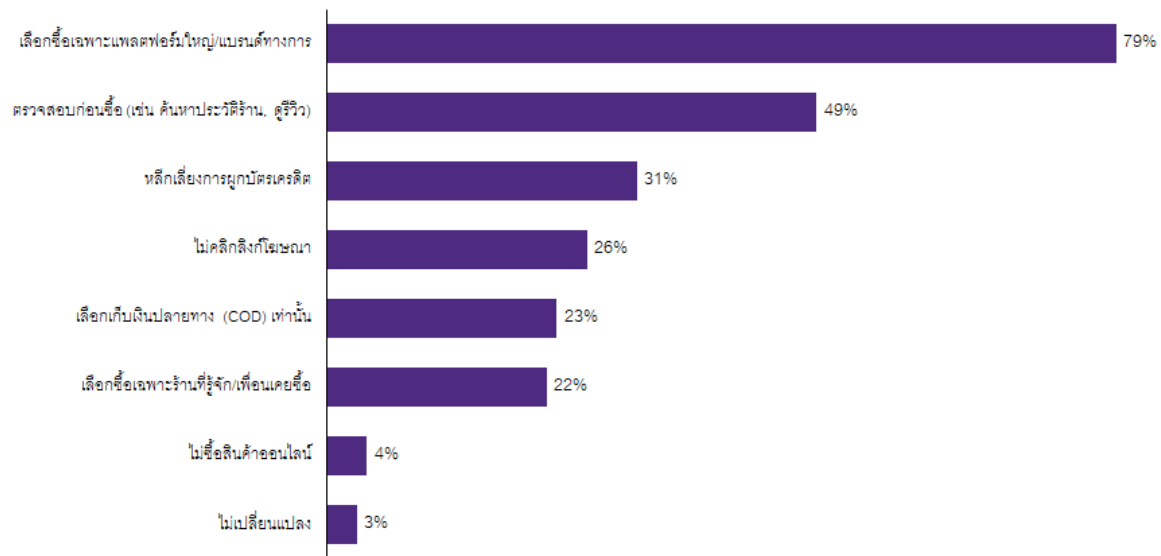


ที่มา : การวิเคราะห์โดย SCB EIC จากข้อมูลของผลสำรวจความคิดเห็นผู้บริโภค “When Life Goes Digital : เทคโนโลยีดิจิทัลมีผลต่อชีวิตคุณอย่างไร?” ในช่วงวันที่ 20 พฤศจิกายน – 11 ธันวาคม 2025

คนไทยส่วนใหญ่เลือกซื้อสินค้าและบริการเฉพาะบนแพลตฟอร์มใหญ่/แบบดั้งเดิมเพื่อหลีกเลี่ยงความเสี่ยงจากการถูกหลอกลวงผ่านการค้าออนไลน์ แม้การซื้อขายและบริการผ่านช่องทางออนไลน์จะมีความเสี่ยงค่อนข้างสูง แต่ปฏิเสธไม่ได้ว่า การซื้อสินค้าและบริการผ่านช่องทางออนไลน์ได้กลายเป็นส่วนหนึ่งของวิถีชีวิตของคนในยุคดิจิทัลไปแล้ว ซึ่งผู้บริโภคได้ปรับเปลี่ยนวิธีการซื้อสินค้าและบริการเพื่อหลีกเลี่ยงความเสี่ยงที่อาจเกิดขึ้น โดยผู้บริโภคกว่า 79% เลือกซื้อสินค้าและบริการเฉพาะบนแพลตฟอร์ม e-Commerce ขนาดใหญ่ที่มีความน่าเชื่อถือหรือซื้อสินค้าและบริการผ่านแพลตฟอร์มทางการของแบรนด์โดยตรงเพื่อเพิ่มความมั่นใจในคุณภาพสินค้าและความปลอดภัยของการทำธุรกรรมทางการเงิน ขณะที่ 49% เลือกใช้ข้อมูลมาประกอบการตัดสินใจโดยให้ความสำคัญกับการตรวจสอบประวัติร้านค้า การอ่านรีวิว หรือความคิดเห็นจากผู้ซื้อรายอื่น และราว 30% หลีกเลี่ยงการผูกบัตรเครดิตหรือผูกข้อมูลบัญชีธนาคารกับแพลตฟอร์มออนไลน์เพื่อลดความเสี่ยงจากการถูกเข้าถึงข้อมูลทางการเงินโดยไม่ได้รับอนุญาต เมื่อเปรียบเทียบพฤติกรรมตามช่วงวัย ยังพบว่า กลุ่ม Gen Z และ Gen Y มีแนวโน้มสูงที่จะเลือกซื้อสินค้าจากร้านค้าที่รู้จักหรือร้านค้าที่เพื่อนแนะนำ ขณะที่กลุ่มผู้สูงอายุวัยเกษียณยังเลือกใช้วิธีการชำระเงินปลายทาง (Cash On Delivery : COD) ในสัดส่วนที่สูงเพื่อหลีกเลี่ยงความเสี่ยงจากการไม่ได้รับสินค้าหากชำระเงินล่วงหน้า

รูปที่ 5 : การปรับเปลี่ยนพฤติกรรมกรรมการซื้อสินค้าและบริการเพื่อหลีกเลี่ยงความเสี่ยงจากสแกมเมอร์

หน่วย : % ของผู้ตอบแบบสอบถามทั้งหมด

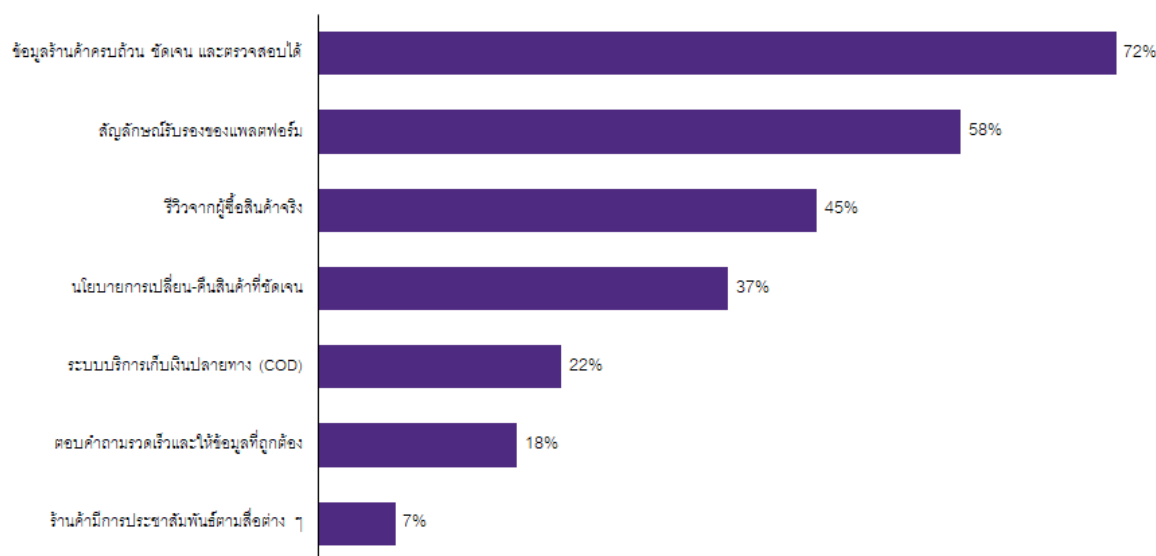


ที่มา : การวิเคราะห์โดย SCB EIC จากข้อมูลของผลสำรวจความคิดเห็นผู้บริโภค “When Life Goes Digital : เทคโนโลยีดิจิทัลมีผลต่อชีวิตคุณอย่างไร?” ในช่วงวันที่ 20 พฤศจิกายน – 11 ธันวาคม 2025

คนไทยเชื่อมั่นและไว้วางใจในร้านค้าออนไลน์ที่ให้ข้อมูลครบถ้วนและตรวจสอบได้ รวมถึงได้รับการรับรองจากแพลตฟอร์ม โดยผลสำรวจของ SCB EIC ยังพบว่า ผู้บริโภคถึง 72% ให้ความสำคัญกับร้านค้าที่มีข้อมูลครบถ้วน ชัดเจน และตรวจสอบได้ ซึ่งรวมถึงข้อมูลผู้ขาย ช่องทางการติดต่อ หรือประวัติการดำเนินธุรกิจ ในขณะเดียวกัน 58% ของผู้บริโภคเชื่อมั่นในตราสัญลักษณ์รับรองร้านค้าที่ออกโดยแพลตฟอร์ม ซึ่งทำหน้าที่เป็นเครื่องยืนยันว่าร้านค้านั้นได้ผ่านกระบวนการตรวจสอบในระดับหนึ่ง นอกจากนี้ 45% ยังใช้ข้อมูลจากการรีวิวของผู้ซื้อสินค้าจริงมาเป็นส่วนประกอบในการตัดสินใจ โดยมองว่าข้อมูลจากประสบการณ์ตรงสะท้อนคุณภาพสินค้าและความน่าเชื่อถือของร้านค้าได้ อีกทั้ง ยังพบว่า กลุ่มผู้สูงอายุวัยเกษียณยังให้ความสำคัญกับนโยบายการเปลี่ยน-คืนสินค้าที่ชัดเจนและเป็นธรรมมากเป็นพิเศษ เพราะช่วยลดความกังวลในกรณีที่เกิดปัญหาหลังการซื้อสินค้า

รูปที่ 6 : ปัจจัยที่จะช่วยสร้างความมั่นใจต่อผู้ขายสินค้าในการซื้อสินค้า/บริการออนไลน์

หน่วย : % ของผู้ตอบแบบสอบถามทั้งหมด



ที่มา : การวิเคราะห์โดย SCB EIC จากข้อมูลของพลสำรวจความคิดเห็นผู้บริโภค “When Life Goes Digital : เทคโนโลยีดิจิทัลมีพลต่อชีวิตคุณอย่างไร?” ในช่วงวันที่ 20 พฤศจิกายน – 11 ธันวาคม 2025

รับมือภัยคุกคามสแกมเมอร์ด้วยการสร้างเกราะป้องกัน

การจัดการกับสแกมเมอร์ให้ลดลงหรือหมดไปนั้นไม่ใช่เรื่องง่ายโดยเฉพาะการหลอกลวงจากการซื้อสินค้าและบริการที่จำนวนผู้ได้รับความเสียหายยังอยู่ในระดับสูง ซึ่งจำเป็นต้องอาศัยความร่วมมือจากทั้งภาครัฐกิจและภาครัฐโดยเน้นการดำเนินมาตรการเชิงรุกควบคู่ไปกับการตรวจสอบและเฝ้าระวังอย่างเป็นระบบเพื่อสร้างความเชื่อมั่นให้กับผู้บริโภค

ธุรกิจ e-Commerce และร้านค้าออนไลน์ต้องยกระดับด้านความปลอดภัยอย่างต่อเนื่อง เพื่อเพิ่มความเชื่อมั่นและความไว้วางใจให้แก่ผู้บริโภค

ปัจจุบัน ผู้ให้บริการแพลตฟอร์ม e-Commerce ได้พัฒนามาตรฐานความปลอดภัยและสร้างกลไกคุ้มครองผู้บริโภคอย่างต่อเนื่อง โดยส่วนใหญ่มุ่งเน้นไปใน 3 แนวทางหลัก ได้แก่ 1. การยกระดับระบบด้วยเทคโนโลยีขั้นสูง ไม่ว่าจะเป็นการนำเทคโนโลยี AI มาใช้ในการตรวจจับกลโกงของสแกมเมอร์ที่แฝงตัวเข้ามา เช่น การใช้ AI มาช่วยสแกนเนื้อหาที่มีความเสี่ยงต่อการหลอกลวง หรือการสร้างระบบแจ้งเตือนให้กับผู้ซื้อสินค้าเมื่อมีการส่งข้อความที่มีความเสี่ยง 2. การคัดกรองร้านค้าอย่างเข้มงวด ผ่านกระบวนการยืนยันตัวตน และการจัดเก็ตร้านค้าหลังผ่านการตรวจสอบข้อมูลอย่างละเอียด โดยปัจจุบันแพลตฟอร์ม e-Commerce รายใหญ่ได้พัฒนาเครื่องหมายรับรองสำหรับร้านค้าที่มีความน่าเชื่อถือซึ่งจะช่วยคัดกรองความเสี่ยงเบื้องต้นให้กับผู้บริโภค 3. การสร้างกลไกคุ้มครองผู้บริโภค เช่น การเพิ่มฟังก์ชันชะลอการจ่ายเงินให้ร้านค้าจนกว่าผู้ซื้อจะได้รับสินค้าและตรวจสอบความถูกต้องภายในเวลาที่กำหนด การเพิ่มขั้นตอนการตรวจสอบและยืนยันตัวตนหลายระดับ (Multi-Factor Authentication : MFA) รวมถึง

การเพิ่มช่องทางด่วนในการรายงาน/แจ้งเหตุเมื่อพบความผิดปกติเพื่อให้แพลตฟอร์มสามารถปิดกั้นร้านค้าที่มีความเสี่ยงได้อย่างทันท่วงทีและดำเนินการตรวจสอบได้อย่างรวดเร็ว อีกทั้ง ยังช่วยลดความเสียหายที่อาจเกิดขึ้น

ในขณะเดียวกัน ร้านค้าหรือธุรกิจที่ต้องการขยายช่องทางการขายสู่ตลาดออนไลน์ควรให้ความสำคัญกับการสร้างความเชื่อมั่นด้านความปลอดภัยแก่ผู้บริโภคด้วยเช่นกัน โดยสามารถพิจารณาแนวทางที่สอดคล้องกับปัจจัยสำคัญที่มีอิทธิพลต่อความเชื่อมั่นของผู้บริโภคจากผลการสำรวจความคิดเห็นผู้บริโภคของ SCB EIC อย่างเช่น

1. **การให้ข้อมูลอย่างครบถ้วน โปร่งใส และตรวจสอบได้** ครอบคลุมทั้งข้อมูลร้านค้า รายละเอียดสินค้า เงื่อนไขการสั่งซื้อ การรับประกันสินค้า รีวิวจากผู้ใช้งาน ค่าใช้จ่ายเพิ่มเติม (หากมี) เช่น ค่าจัดส่ง หรือค่าธรรมเนียม ตลอดจนช่องทางการติดต่อร้านค้าที่หลากหลาย เช่น แชนแนล กล้องข้อความ (Inbox) โทรศัพท์ หรืออีเมล ที่สามารถตอบสนองได้รวดเร็ว รวมถึงระบบการให้บริการหลังการขายที่สามารถช่วยแก้ไขปัญหาของลูกค้าได้อย่างทันท่วงทีและมีประสิทธิภาพ

2. **การกำหนดนโยบายคุ้มครองผู้บริโภคที่น่าเชื่อถือ ชัดเจน โปร่งใส และเป็นธรรม** เช่น การกำหนดเงื่อนไขรับประกันความพึงพอใจในสินค้าและบริการ นโยบายการจัดส่งสินค้า นโยบายการคืนเงินหรือเปลี่ยนสินค้าในกรณีที่สินค้าชำรุดหรือไม่ตรงตามโฆษณา รวมถึงการชดเชยเมื่อเกิดปัญหาหรือเกิดความผิดพลาดในการจัดส่ง

3. **การนำเทคโนโลยีด้านความปลอดภัยมาใช้** ไม่ว่าจะเป็นระบบรักษาความปลอดภัยทางไซเบอร์ (Cyber security) และระบบคุ้มครองความปลอดภัยของข้อมูลส่วนบุคคลเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและลดความเสี่ยงจากภัยคุกคามทางออนไลน์ รวมถึงการใช้ระบบการชำระเงินที่ได้มาตรฐานผ่านผู้ให้บริการชำระเงินที่ได้รับการรับรองในระดับสากลเพื่อสร้างความมั่นใจให้แก่ผู้บริโภคในทุกขั้นตอนการซื้อสินค้า

ในขณะเดียวกัน ภาครัฐได้กำหนดให้การปราบปรามสแกมเมอร์เป็น “วาระแห่งชาติ” และเร่งดำเนินมาตรการเชิงรุกในหลายมิติ อย่างไรก็ตาม อาจพิจารณายกระดับความเข้มข้นของมาตรการเพื่อให้การป้องกันและปราบปรามภัยจากสแกมเมอร์มีประสิทธิภาพยิ่งขึ้น อย่างเช่น

1. **การออกกฎหมายที่เข้มงวดและครอบคลุมมากขึ้น** ปัจจุบันไทยใช้ พ.ร.ก. มาตรการป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยี พ.ศ. 2566 เป็นเครื่องมือหลักในการปราบปรามสแกมเมอร์ โดยนอกจากการกระทำของสแกมเมอร์จะถูกดำเนินคดีแล้ว กฎหมายยังอนุญาตให้ผู้เสียหายแจ้งธนาคารระงับบัญชีที่เกี่ยวข้องได้ทันที รวมถึงกำหนดบทลงโทษผู้ที่ยินยอมให้ผู้อื่นใช้บัญชีเงินฝากหรือบัญชีม้า อย่างไรก็ตาม ภาครัฐอาจพิจารณาขยายกรอบกฎหมายเพิ่มความรับผิดชอบให้แก่ภาคธุรกิจที่เกี่ยวข้องในกรณีที่ละเลยมาตรการป้องกันการฉ้อโกง หรือระบบรักษาความปลอดภัยที่ไม่มีประสิทธิภาพเพียงพอจนเป็นช่องทางให้สแกมเมอร์สร้างความเสียหายแก่ผู้บริโภค ตัวอย่างเช่น รัฐบาลออกสตรเลียมออกกฎหมายโทษปรับสูงสุดถึง 50 ล้านดอลลาร์ออสเตรเลีย หากพิสูจน์ได้ว่าภาคธุรกิจมีความบกพร่องในการป้องกันการหลอกลวง อีกทั้ง ยังกำหนดมาตรการชดเชยความเสียหาย โดยให้ผู้เสียหายมีสิทธิได้รับเงินคืนหรือค่าชดเชยจากแพลตฟอร์มดิจิทัลที่ระบบความปลอดภัยไม่มีประสิทธิภาพ

2. **การยกระดับการบูรณาการข้อมูลและการปฏิบัติงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง** ปัจจุบันไทยได้จัดตั้งศูนย์ปฏิบัติการเฉพาะกิจเพื่อป้องกันและปราบปรามอาชญากรรมทางเทคโนโลยีในการรับแจ้งเหตุ ระงับบัญชีม้า

และสกัดกันเส้นทางการเงินของสแกมเมอร์ รวมถึงสร้างระบบฐานข้อมูลที่เชื่อมโยงข้อมูลระหว่างหน่วยงานภาครัฐ สถาบันการเงิน และภาคธุรกิจเข้าด้วยกัน อย่างไรก็ดี ภาครัฐอาจพิจารณายกระดับความร่วมมือเชิงปฏิบัติการเพิ่มเติม ผ่านการจัดตั้งคณะทำงานที่มีเจ้าหน้าที่ภาครัฐ สถาบันการเงิน และผู้ให้บริการแพลตฟอร์มเทคโนโลยีเข้ามาทำงาน ร่วมกัน ซึ่งเป็นแนวทางเดียวกับสิงคโปร์ที่มุ่งเน้นการบูรณาการข้อมูลและความร่วมมือระหว่างหน่วยงานในการรับมือ ปัญหาสแกมเมอร์ และยังช่วยเพิ่มประสิทธิภาพในการตรวจจับและระงับภัยคุกคามได้อย่างทันท่วงทีแบบเรียลไทม์ มากยิ่งขึ้น

3. การประยุกต์ใช้เทคโนโลยีสมัยใหม่ในการป้องกันและแจ้งเตือนภัย โดยไทยได้เริ่มนำเทคโนโลยีขั้นสูงมาใช้ในการปราบปรามสแกมเมอร์แล้วทั้งเทคโนโลยี AI และระบบ Data Bureau ในการวิเคราะห์ข้อมูลธุรกรรมทางการเงินเพื่อ สกัดกันเส้นทางการเงินของสแกมเมอร์ ซึ่งภาครัฐอาจพิจารณานำเทคโนโลยีขั้นสูงมาใช้เพิ่มเติมในการพัฒนาเครื่องมือ ป้องกันภัยให้แก่ประชาชน แนวทางนี้สอดคล้องกับแนวทางของรัฐบาลจีนที่พัฒนาแอปพลิเคชันเตือนภัยระดับชาติ ภายใต้การกำกับของกระทรวงความมั่นคงสาธารณะที่จะช่วยลดโอกาสที่ประชาชนจะตกเป็นเหยื่อของการฉ้อโกง โดยใช้เทคโนโลยี AI เข้ามาตรวจจับสัญญาณโทรศัพท์เข้า ข้อความ แอปพลิเคชันแปลกปลอม รวมถึงการตรวจจับ พฤติกรรมเสี่ยงที่เข้าข่ายการถูกหลอกลวง

ทั้งนี้สแกมเมอร์ยังคงเป็นภัยร้ายที่แทรกซึมอยู่ในชีวิตดิจิทัลของคนไทยอย่างต่อเนื่อง โดยอาศัย ความก้าวหน้าทางเทคโนโลยีและพฤติกรรมการใช้งานออนไลน์ที่เพิ่มขึ้นในการหลอกลวงจนนำไปสู่ ความเสียหายในวงกว้าง ปัญหาดังกล่าวสะท้อนให้เห็นถึงความจำเป็นในการร่วมมือกันระหว่างภาครัฐ และภาคธุรกิจเพื่อยกระดับมาตรการป้องกันและสร้างความปลอดภัยในสังคมดิจิทัลไทย

บทวิเคราะห์โดย... <https://www.scbeic.com/th/detail/product/Scammer-280826>

Disclaimer: This article is made by The Siam Commercial Bank ("SCB") for the purpose of providing information and analysis only. Any information and analysis herein are collected and referred from public sources which may include economic information, marketing information or any reliable information prior to the date of this document. SCB makes no representation or warranty as to the accuracy, completeness and up-to-dateness of such information and SCB has no responsibility to verify or to proceed any action to make such information to be accurate, complete, and up-to-date in any respect. The information contained herein is not intended to provide legal, financial or tax advice or any other advice, and it shall not be relied or referred upon proceeding any transaction. In addition, SCB shall not be liable for any damages arising from the use of information contained herein in any respect.

ผู้เชี่ยวชาญวิเคราะห์

ดร.กมลมาลย์ แจ่งล้อม (kamonmarn.jaenglom@scb.co.th)

นักวิเคราะห์อาวุโส

INDUSTRY ANALYSIS

ดร. ยรรยง ไทยเจริญ

ประธานเจ้าหน้าที่บริหาร สายงานวิจัยเศรษฐกิจและความยั่งยืน ศูนย์วิจัยเศรษฐกิจและธุรกิจ (SCB EIC)

ปราณีดา ศยามานนท์

ผู้อำนวยการ ฝ่ายบริหารฝ่าย Industry Analysis

ดร.กมลมาลย์ แจ่งล้อม

นักวิเคราะห์อาวุโส

บุณยภพ ดันตปิฎก

นักวิเคราะห์อาวุโส

กิริติญา ครองแก้ว

นักวิเคราะห์อาวุโส

จิรุตม์ อัมรัตน์

นักวิเคราะห์อาวุโส



ท่านพึงพอใจต่อบทวิเคราะห์นี้เพียงใด?

ความเห็นของท่าน สำคัญกับเรา

ร่วมตอบแบบสอบถาม 7 ข้อ
เพื่อนำไปพัฒนามาตรการของ
SCB EIC ต่อไป

คลิกเพื่อทำ
แบบสอบถาม



“Economic and business
intelligence for effective
decision making”



ECONOMIC INTELLIGENCE CENTER

ศูนย์วิจัยเศรษฐกิจและธุรกิจ ธนาคารไทยพาณิชย์



เจาะลึก

สถานการณ์เศรษฐกิจ



เกาะติด

การเปลี่ยนแปลงที่ส่งพล
ต่อภาคธุรกิจ



อัปเดต

ประเด็นร้อนที่ไม่ควรพลาด



Stay connected

Find us at



@scbeic | 🔍

www.scbeic.com