ความมั่นคงปลอดภัยบนอินเตอร์เน็ตและการปฏิบัติตนสำหรับข้าราชการยุคดิจิทัล

สรุปสาระสำคัญ

ตอนที่ ๑ สถานการณ์การใช้อินเตอร์เน็ตและการเปลี่ยนแปลงต่าง ๆ

- **แนวโน้มการใช้งานอินเตอร์เน็ตในประเทศไทย**

๑. การเข้าถึงและการใช้งานที่ครอบคลุม

สัดส่วนผู้ใช้: ประชากรไทยเข้าถึงอินเทอร์เน็ตสูงถึง ๙๑.๒% - ๙๔.๗% หรือประมาณ ๖๕-๖๗ ล้านคน ซึ่งสูงกว่าค่าเฉลี่ยโลกอย่างมีนัยสำคัญ

๒. แพลตฟอร์มและกิจกรรมยอดนิยม

โซเชียลมีเดีย: แพลตฟอร์มที่ครองใจคนไทยอันดับต้นๆ คือ Facebook (๙๐.๗%), LINE (๙๐.๖%) และ TikTok (๘๕.๗%) โดย TikTok มีอัตราการเติบโตที่โดดเด่นที่สุด

๓. เทคโนโลยีและเศรษฐกิจดิจิทัล

AI และ Mobile First: การใช้ AI เริ่มกลายเป็นส่วนหนึ่งของชีวิตประจำวัน และการชำระเงินดิจิทัลอย่าง Prompt Pay มีการใช้งานสูงถึง ๗๑ ล้านรายการต่อวัน

- **สถิติการใช้งานของประเทศไทย**

ภาพรวมการเข้าถึงอินเทอร์เน็ตจำนวนผู้ใช้งาน: มีผู้ใช้อินเทอร์เน็ตในไทยประมาณ ๖๗.๘ ล้านคน คิดเป็นสัดส่วนสูงถึง ๙๔.๗% ของประชากรทั้งหมด

- **ความสัมพันธ์และการกระจายตัวของข้อมูล**

๑. การกระจายตัวเชิงพื้นที่ (Geographic Distribution) แม้การเข้าถึงภาพรวมจะสูงถึง ๙๔.๗% แต่สัดส่วนการเชื่อมต่อยังมีความแตกต่างกันตามภูมิภาค ด

๒. ความสัมพันธ์ตามช่วงวัย (Demographic Correlation) พฤติกรรมการใช้งานมีความสัมพันธ์อย่างมากกับอายุ (Generation):Gen Z (๖-๒๔ ปี): มีสัดส่วนการใช้อินเทอร์เน็ตสูงสุดเกือบเต็มจำนวนที่ ๙๘.๒% Gen Y (๒๕-๔๒ ปี): เป็นกลุ่มที่มีความสัมพันธ์กับการใช้งานเชิงเศรษฐกิจสูงสุด เช่น การทำธุรกรรมออนไลน์และ E-government servicesผู้สูงอายุ (๖๐ ปีขึ้นไป): แม้จะมีการใช้งานเพิ่มขึ้นเป็น ๖๒.๑% แต่ยังคงมีความสัมพันธ์กับข้อจำกัดด้านทักษะดิจิทัล

๓. ปัจจัยที่ส่งผลต่อการเข้าถึงข้อมูล เพศ: ข้อมูลปี ๒๕๖๘ ชี้ว่าเพศชายมีสัดส่วนการใช้อินเทอร์เน็ต (๙๒.๐%) สูงกว่าเพศหญิงเล็กน้อย (๘๙.๘%)ระดับการศึกษา: มีความสัมพันธ์เชิงบวกสูงสุดกับการใช้งานบริการดิจิทัล โดยผู้ที่มีการศึกษาระดับปริญญาตรีขึ้นไปมีแนวโน้มใช้งานเชิงลึกมากกว่ากลุ่มอื่น

- **วิวัฒนาการของเวบไซต์**

๑. Web ๑.๐ (Static Web) - ยุคแห่งการอ่าน (๑๙๙๐ - ๒๐๐๔)ลักษณะ: เว็บไซต์เป็นแบบ "สื่อสารทางเดียว" เหมือนอ่านหนังสือพิมพ์ออนไลน์ World Wide Web ยุคแรกมีเพียงข้อความและภาพนิ่งเทคโนโลยี: ใช้ HTML พื้นฐาน ผู้ใช้ทำได้เพียงอ่านข้อมูล ไม่สามารถโต้ตอบหรือคอมเมนต์ได้พฤติกรรม: เป็นเพียงผู้รับสาร (Passive User)

๒. Web ๒.๐ (Social Web) - ยุคแห่งการโต้ตอบ (๒๐๐๔ - ปัจจุบัน) ลักษณะ: เว็บไซต์เน้น "การมีส่วนร่วม" และ "เนื้อหาจากผู้ใช้" (User-Generated Content) จุดเปลี่ยน: เกิดแพลตฟอร์มอย่าง Facebook, YouTube และ Wikipedia ที่เปิดให้คนไทยเข้าไปสร้างคอนเทนต์เองความสัมพันธ์: สอดคล้องกับสถิติที่คนไทยใช้โซเชียลมีเดียถึง ๗๙.๑% เพราะเน้นการเชื่อมต่อและแบ่งปันข้อมูล

๓. Web ๓.๐ (Semantic Web) - ยุคแห่งปัญญาประดิษฐ์ (ปัจจุบัน - อนาคต) ลักษณะ: เว็บไซต์ "ฉลาด" ขึ้นด้วย AI และ Machine Learning ที่เข้าใจความหมายของข้อมูล (Contextual Understanding)จุดเด่น:Personalization: เว็บจะแสดงเนื้อหาที่ออกแบบมาเพื่อ "เรา" โดยเฉพาะ (เช่น หน้าฟีด TikTok ของแต่ละคน)Decentralization: การมาของ Blockchain และสินทรัพย์ดิจิทัลที่ลดการพึ่งพาตัวกลางพฤติกรรม: ข้อมูลถูกกระจายตัวตามความสนใจเฉพาะบุคคล (Niche Markets) มากขึ้น

๔. Web ๔.๐ (The Intelligent/Symbiotic Web) - ยุคไร้รอยต่อทิศทาง: เป็นยุคที่อินเทอร์เน็ตเชื่อมต่อกับทุกสิ่ง (IoT) และมนุษย์อย่างสมบูรณ์ เช่น การสั่งงานด้วยเสียงผ่าน Siri หรือการใช้ Generative AI ช่วยตัดสินใจแบบ Real-time ซึ่งสอดคล้องกับเทรนด์ Smart Home ในไทยที่กำลังเติบโต

ตอนที่ ๒ การกระทำความผิดทางคอมพิวเตอร์และสิ่งที่ต้องพึงระวัง

- **รูปแบบและลักษณะการกระทำความผิดทางคอมพิวเตอร์**

๑. การหลอกลวงออนไลน์ (Online Fraud & Scams) นี่คือรูปแบบที่พบบ่อยที่สุดในไทย โดยสัมพันธ์กับพฤติกรรม Social Commerce ที่สูงขึ้น:Phishing: การสร้างเว็บไซต์ปลอมหรืออีเมลปลอมเพื่อหลอกเอาข้อมูลส่วนตัว (เช่น รหัสผ่าน Mobile Banking)

๒. การเข้าถึงข้อมูลโดยมิชอบ (Hacking & Data Breach) ในยุคที่ข้อมูลคือขุมทรัพย์ การโจมตีเป้าหมายไปที่ฐานข้อมูลเป็นเรื่องวิกฤต: Illegal Access: การลักลอบเข้าสู่ระบบคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาต Ransomware: การใช้มัลแวร์เรียกค่าไถ่เพื่อล็อกข้อมูลขององค์กร ซึ่งสอดคล้องกับแนวโน้มการขยายตัวของระบบ Cloud Computing ในไทยที่ต้องระวังความปลอดภัยมากขึ้น

๓. การนำเข้าข้อมูลที่ผิดกฎหมาย (Illegal Content) ตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ของไทย มีลักษณะเด่นดังนี้: Fake News: การนำเข้าข้อมูลเท็จที่น่าจะก่อให้เกิดความเสียหายต่อประชาชนหรือความมั่นคง Computer-related Defamation: การตัดต่อภาพหรือการเผยแพร่ข้อมูลที่ทำให้ผู้อื่นเสียชื่อเสียง ซึ่งมักเกิดบนแพลตฟอร์มยอดนิยมอย่าง Facebook และ TikTok

๔. การละเมิดสิทธิและข้อมูลส่วนบุคคล ด้วยการประกาศใช้ PDPA (Personal Data Protection Act), การเก็บหรือใช้ข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมถือเป็นความผิดร้ายแรง ซึ่งสัมพันธ์กับการกระจายตัวของข้อมูลในยุค Big Data

- **สิ่งที่ต้องพึงระวังในการใช้งานบนอินเตอร์เน็ต**

๑. การรักษาความเป็นส่วนตัวและข้อมูลส่วนบุคคล (Privacy & PDPA)ในยุคที่ข้อมูลกระจายตัวอยู่ทั่วไป การปกป้องข้อมูลคือด่านแรก:ตรวจสอบสิทธิ์ (App Permissions): ก่อนติดตั้งแอปพลิเค

ชัน ควรตรวจสอบว่าแอปขอเข้าถึงข้อมูลที่ไม่จำเป็นหรือไม่ การแชร์ข้อมูลสาธารณะ: หลีกเลี่ยงการโพสต์ภาพตั๋วเครื่องบิน บัตรประชาชน หรือตำแหน่งที่ตั้งแบบ Real-time บน Facebook หรือ TikTok เพราะอาจถูกนำไปใช้ในทางที่ผิดหรือเป็นช่องทางให้มิจฉาชีพติดตามตัวได้

๒. การตรวจสอบความน่าเชื่อถือของแหล่งข้อมูล (Information Verification) เนื่องจากคนไทยใช้เน็ตเพื่อ "ค้นหาข้อมูล" เป็นอันดับ ๑ จึงเสี่ยงต่อ Fake News:Check Before Share: ตรวจสอบที่มาของข่าวสารจากแหล่งที่เชื่อถือได้ เช่น ศูนย์ต่อต้านข่าวปลอม (Anti-Fake News Center Thailand) ก่อนกดแชร์ทุกครั้ง

๓. ความปลอดภัยในการทำธุรกรรมทางการเงิน (Financial Security)สอดคล้องกับสถิติการใช้ Digital Payment ที่สูงติดอันดับโลก:หลีกเลี่ยง Public Wi-Fi: ห้ามทำธุรกรรมการเงินหรือล็อกอินบัญชีสำคัญผ่าน Wi-Fi สาธารณะที่ไม่มีการป้องกันรหัสผ่าน

๔. มารยาทและการใช้สิทธิบนโลกออนไลน์ (Digital Citizenship) Cyberbullying: การแสดงความคิดเห็นที่รุนแรงหรือการคุกคามผู้อื่นอาจมีความผิดตาม พ.ร.บ. คอมพิวเตอร์ฯลิขสิทธิ์ทางปัญญา: การนำรูปภาพหรือวิดีโอของผู้อื่นมาใช้ในเชิงพาณิชย์โดยไม่ได้รับอนุญาต ถือเป็นการละเมิดกฎหมายที่มีบทลงโทษชัดเจน

๕. การระวังภัยจาก Generative AI ในยุคที่ AI พัฒนาไปไกล ต้องระวัง Deepfake หรือการปลอมแปลงเสียงและใบหน้าเพื่อใช้ในการหลอกลวง (Impersonation Scam) ซึ่งเริ่มพบมากขึ้นในประเทศไทย

- **พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์**

๑. ฐานความผิดเกี่ยวกับระบบและข้อมูลคอมพิวเตอร์ การเข้าถึงโดยมิชอบ (Hacking): การแอบเข้าเครื่องคอมพิวเตอร์หรือระบบของผู้อื่นที่มีมาตรการป้องกันไว้ (มาตรา ๕-๘) การแก้ไขดัดแปลงข้อมูล: การทำให้ข้อมูลของผู้อื่นเสียหาย ทำลาย แก้ไข หรือระงับข้อมูลคอมพิวเตอร์โดยมิชอบ (มาตรา ๙-๑๐)การรบกวนระบบ (DoS/DDoS): การกระทำที่ทำให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถใช้งานได้ตามปกติ (มาตรา ๑๐)

๒. ฐานความผิดเกี่ยวกับเนื้อหา (Content-related Offenses) นี่คือส่วนที่เกี่ยวข้องกับผู้ใช้งานทั่วไปมากที่สุดในยุค Social Media: ข้อมูลเท็จ/ข่าวปลอม (มาตรา ๑๔): การนำเข้าข้อมูลปลอมหรือข้อมูลที่บิดเบือน ซึ่งกระทบต่อความมั่นคง ปริการสาธารณะ หรือสร้างความตื่นตระหนก (สอดคล้องกับเรื่อง Fake News ที่ต้องระวัง)ข้อมูลลามก (มาตรา ๑๔(๔)): การนำเข้าข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะอันลามกและประชาชนทั่วไปเข้าถึงได้การตัดต่อภาพ (มาตรา ๑๖): การนำภาพผู้อื่นมาตัดต่อ ดัดแปลง เพื่อทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น หรือได้รับความอับอาย

๓. มาตราสำคัญที่เป็นเรื่องใกล้ตัว Spam (มาตรา ๑๑): การส่งอีเมลหรือข้อความรบกวนผู้อื่นโดยไม่เปิดโอกาสให้บอกเลิกหรือปฏิเสธได้ง่าย (เช่น การฝากร้านใน IG/Facebook โดยที่เจ้าของไม่ยินยอม) ความรับผิดของผู้ให้บริการ (มาตรา ๑๕): แพลตฟอร์มหรือแอดมินเพจต้องรับผิดชอบหากให้ความร่วมมือหรือยินยอมให้มีข้อมูลผิดกฎหมายอยู่ในระบบ (แต่หากพิสูจน์ได้ว่าดำเนินการลบตามขั้นตอนจะได้รับยกเว้นโทษ)

๔. ความสัมพันธ์กับกฎหมายอื่น ปัจจุบันมีการนำ พ.ร.บ. คอมพิวเตอร์ฯ มาใช้งานร่วมกับ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) เพื่อดูแลเรื่องการละเมิดสิทธิและความปลอดภัยทางไซเบอร์ ให้ครอบคลุมยิ่งขึ้นบทลงโทษ มีตั้งแต่โทษปรับหลักหมื่นไปจนถึงหลักแสนบาท และโทษจำคุกตั้งแต่ ๑ ปี ถึง ๒๐ ปี ขึ้นอยู่กับความร้ายแรงของความผิดที่กระทำ

ตอนที่ ๓ ตัวอย่างสิ่งที่เกิดขึ้นบนโลกออนไลน์

- **การใช้โปรแกรมและการบริโภคข้อมูลโดยขาดความยั้งคิด**

๑. กับดักของอัลกอริทึม (The Algorithm Trap) Echo Chamber: เมื่ออัลกอริทึมของแพลตฟอร์มอย่าง TikTok หรือ Facebook เลือกแสดงเฉพาะข้อมูลที่ตรงกับความชอบของเรา จะทำให้เราขาดการเปิดรับข้อมูลรอบด้าน และเกิดความเชื่อที่รุนแรงขึ้น (Polarization)Filter Bubble: การถูกตีกรอบข้อมูลโดยไม่รู้ตัว ทำให้เกิดความสัมพันธ์ที่ผิดเพี้ยนระหว่าง ความจริง กับ สิ่งที่หน้าจอนำเสนอ

๒. ผลกระทบต่อกระบวนการคิดและจิตใจ Information Overload: การรับข้อมูลที่ล้นหลามเกินความจำเป็น (ตามสถิติคนไทยเล่นเน็ตเกือบ ๘ ชม./วัน) ส่งผลให้เกิดภาวะ "สมองล้า" และความสามารถในการตัดสินใจอย่างมีวิจารณญาณลดลงDopamine Loop: การใช้งานแอปพลิเคชันที่ออกแบบมาเพื่อดึงดูดความสนใจ (Infinite Scroll) ทำให้เราเสพติดการกระตุ้นระยะสั้น จนขาดสมาธิในการทำงานหรือเรียนรู้เชิงลึก

๓. ความเสี่ยงทางกฎหมายและอาชญากรรม (พ.ร.บ. คอมพิวเตอร์ฯ) การ "ขาดความยั้งคิด" มักนำไปสู่ความผิดตามกฎหมายที่คุณเพิ่งศึกษาไป: การแชร์ข้อมูลทันที (Instant Share): การแชร์ข่าวปลอมหรือข้อมูลที่บิดเบือนโดยไม่ตรวจสอบแหล่งที่มา อาจเข้าข่ายความผิด มาตรา ๑๔ ของ พ.ร.บ. คอมพิวเตอร์ฯ การแสดงความเห็นด้วยอารมณ์: การพิมพ์ด่าทอหรือตัดต่อภาพผู้อื่นเพียงเพื่อความสนุกชั่ววูบ อาจนำไปสู่คดีหมิ่นประมาททางคอมพิวเตอร์

๔. การใช้โปรแกรมโดยไม่ระวังความปลอดภัย Shadow IT: การดาวน์โหลดโปรแกรมหรือแอปพลิเคชันเถื่อนเพียงเพราะต้องการใช้งานฟรี สุ่มเสี่ยงต่อการถูกฝังมัลแวร์เรียกค่าไถ่ (Ransomware) ซึ่งเป็นภัยคุกคามอันดับต้นๆ ในปัจจุบัน

- **ตัวอย่าง Hacking Wi Fi User Euro Grabber**

๑. ลักษณะการทำงาน (The Mechanism) Euro grabber ไม่ใช่แค่การแฮ็ก Wi-Fi ทั่วไป แต่เป็นมัลแวร์ระดับสูงที่เคยโจมตีระบบธนาคารในยุโรป โดยเริ่มจากการหลอกให้ผู้ใช้ติดตั้งมัลแวร์ลงในคอมพิวเตอร์ (มักมากับโปรแกรมเถื่อนหรืออีเมลหลอกลวง)เมื่อผู้ใช้ล็อกอิน Mobile Banking ผ่านเครือข่ายอินเทอร์เน็ต มัลแวร์จะส่ง SMS หลอกลวงให้ติดตั้งแอปบนมือถือซ้ำ เพื่อดักจับรหัส OTP (One-Time Password)

๒. ความเสี่ยงและผลกระทบ (Impact) ความสูญเสียทรัพย์สิน: ในอดีตกรณี Euro grabber สามารถขโมยเงินจากบัญชีผู้ใช้ไปได้รวมกว่า ๓๖ ล้านยูโร (ประมาณ ๑,๓๐๐ ล้านบาท)การเข้าถึงข้อมูลโดยมิชอบ: ถือเป็นความผิดชัดเจนตาม พ.ร.บ. คอมพิวเตอร์ฯ มาตรา ๕-๘ ว่าด้วยการเข้าถึงระบบและข้อมูลโดยมิชอบ และมาตรา ๑๒ หากกระทบต่อความมั่นคงทางเศรษฐกิจ

๓. วิธีป้องกันตามหลักความปลอดภัย (Best Practices) หลีกเลี่ยง Wi-Fi สาธารณะ: ไม่ควรทำธุรกรรมการเงินผ่าน Wi-Fi ที่ไม่ได้เข้ารหัสรหัสผ่าน (Open Wi-Fi)สังเกตความผิดปกติของ Browser: หากเว็บไซต์ธนาคารมีการขอให้ติดตั้งซอฟต์แวร์เพิ่มเติม หรือขอเบอร์โทรศัพท์ซ้ำซ้อนเพื่อส่งลิงก์ติดตั้งแอป ให้สันนิษฐานว่าเป็นมัลแวร์

๔. บทลงโทษตามกฎหมายไทย หากมีการกระทำดังกล่าวในประเทศไทย ผู้กระทำผิดจะได้รับโทษหนักภายใต้ พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ทั้งโทษจำคุกและปรับ รวมถึงอาจโดนคดีฉ้อโกงประชาชนเพิ่มเติมด้วย

- **ตัวอย่าง Web Defacement ไวรัสเรียกค่าไถ่ ตัวอย่าง Hot Hot**

เป็นการโจมตีที่มักมีวัตถุประสงค์เพื่อประกาศชัยชนะ ลบหลู่ หรือแสดงสัญลักษณ์บางอย่าง ซึ่งผิดตาม พ.ร.บ. คอมพิวเตอร์ฯ มาตรา ๙

ตอนที่ ๔ วิธีป้องกันและตรวจสอบความปลอดภัยด้วยตนเอง

- **การตั้งค่าความปลอดภัยสำหรับ Facebook**

๑. เปิดการยืนยันตัวตนสองชั้น (Two-Factor Authentication - ๒FA) นี่คือเกราะป้องกันที่สำคัญที่สุด แม้แฮ็กเกอร์จะรู้รหัสผ่าน แต่ก็เข้าไม่ได้ถ้าไม่มีรหัสจากมือถือ

๒. ตรวจสอบการเข้าสู่ระบบ (Where You're Logged In) เพื่อเช็กว่ามีอุปกรณ์แปลกปลอม (ของแฮ็กเกอร์) แอบใช้งานบัญชีอยู่หรือไม่

๓. เปิดการแจ้งเตือนการเข้าสู่ระบบ (Login Alerts)ความสำคัญ: เมื่อมีการล็อกอินจากบราวเซอร์หรืออุปกรณ์ใหม่ Facebook จะส่งข้อความแจ้งเตือนทันที ช่วยให้ไหวตัวทันก่อนเกิดเหตุ Web Defacement หรือการสวมรอยโพสต์ข้อมูลเท็จ

๔. จำกัดการเข้าถึงข้อมูลส่วนตัว (Privacy Checkup) เพื่อป้องกันมิจฉาชีพนำข้อมูลไปใช้ทำ Social Engineering หรือหลอกลวงคนใกล้ชิด

๕. ระวัง "แอปภายนอก" (Apps and Websites)หลายคน "ขาดความยั้งคิด" โดยใช้ Facebook ไปล็อกอินเว็บดูหนังหรือแอปเกมส์เถื่อน

- **การตั้งค่าความปลอดภัยสำหรับ Gmail**

๑. การตรวจสอบความปลอดภัย (Security Checkup)

๒. เปิดการยืนยันตัวตนสองชั้น (๒-Step Verification)

๓. ตรวจสอบการเข้าถึงของแอปภายนอก (Third-party apps)

๔. ตั้งค่าอีเมลและเบอร์โทรศัพท์สำรอง (Recovery Info)

๕. เปิดโหมดการใช้งานที่ปลอดภัยยิ่งขึ้น (Enhanced Safe Browsing)

- **การตั้งค่าความปลอดภัยสำหรับ LINE**

๑. ตรวจสอบอุปกรณ์ที่เข้าสู่ระบบ (Logged-in Devices) มิจฉาชีพมักแอบล็อกอินบัญชีผ่าน PC หรือ iPad โดยที่ไม่รู้ตัว วิธีตั้งค่า: ไปที่หน้าหลัก > ตั้งค่า (รูปฟันเฟือง) > บัญชี > อุปกรณ์ที่เข้าสู่ระบบ สิ่งที่ต้องทำ: หากพบอุปกรณ์แปลกปลอม ให้กด "ออกจากระบบ" ทันที และรีบเปลี่ยนรหัสผ่าน
๒. ปิดการอนุญาตให้เข้าสู่ระบบจากอุปกรณ์อื่น (Allow Login) หากใช้งาน LINE แค่บนมือถือเครื่องเดียว แนะนำให้ปิดฟีเจอร์นี้เพื่อบล็อกการแฮ็กจากทางไกลวิธีตั้งค่า: ในหน้า บัญชี ให้ปิดเมนู "อนุญาต

ให้เข้าสู่ระบบ" (Allow Login) ผลลัพธ์: จะไม่มีใครสามารถล็อกอินบัญชีบนคอมพิวเตอร์หรือแท็บเล็ตได้เลย

๓. เปิดใช้งานการเข้ารหัสลับขั้นสูง (Letter Sealing) ฟีเจอร์นี้ช่วยให้ข้อความถูกอ่านได้เฉพาะตัวและคู่สนทนาเท่านั้น ป้องกันการถูกดักฟังข้อมูล (Man-in-the-Middle) แบบกรณี Euro Grabber วิธีตั้งค่า: ไปที่ ตั้งค่า > ความเป็นส่วนตัว > ตรวจสอบให้แน่ใจว่าเปิด "Letter Sealing" ไว้แล้ว

๔. ปฏิเสธการรับข้อความจากคนที่ไม่ใช่เพื่อน (Filter Messages) เพื่อป้องกัน SMS/Link หลอกลวง หรือ Fake News จากมิจฉาชีพที่ไม่ได้เป็นเพื่อนกับเรา วิธีตั้งค่า: ไปที่ ตั้งค่า > ความเป็นส่วนตัว > เปิด "ปฏิเสธการรับข้อความ" (Filter Messages)

๕. ตั้งรหัสล็อกแอป (Passcode Lock) ป้องกันกรณีมือถือถูกขโมย หรือมีคนแอบมาเปิดอ่านแอป LINE ของคุณโดย ขาดความยั้งคิด วิธีตั้งค่า: ไปที่ ตั้งค่า > ความเป็นส่วนตัว > เปิด "ล็อกรหัสผ่าน"