สรุปผลการพัฒนาความรู้
โครงการพัฒนาบุคลากรด้านคอมพิวเตอร์และสารสนเทศ
หลักสูตร “การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ”
วันอังคารที่ ๓๑ มกราคม ๒๕๖๖
ณ ห้องปฏิบัติการฝึกอบรมคอมพิวเตอร์และภูมิสารสนเทศ
จัดโดย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมพัฒนาที่ดิน

บรรยายโดย นายอาทิตย์ ซื่อสัตย์สิทธิกร

<u>พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒</u>

มีผลบังคับใช้เมื่อวันที่ ๑ มิถุนายน ๒๕๖๕ ซึ่งเหตุผลที่ประกาศใช้พระราชบัญญัตินี้ เนื่องจากปัจจุบันมีการล่วงละเมิดสิทธิความเป็นส่วนตัวของข้อมูลส่วนบุคคลเป็นจำนวนมากจนสร้างความเดือดร้อนรำคาญหรือความเสียหายให้แก่เจ้าของข้อมูลส่วนบุคคล ประกอบกับความก้าวหน้าของเทคโนโลยีทำให้การเก็บรวมรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลอันเป็นการล่วงละเมิดดังกล่าว ทำได้โดยง่าย สะดวก และ รวดเร็ว ก่อให้เกิดความเสียหายต่อเศรษฐกิจโดยรวม สมควรกำหนดให้มีกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคลเป็นการทั่วไปขึ้น เพื่อกำหนดหลักเกณฑ์ กลไก หรือมาตรการกำกับดูแลเกี่ยวกับการให้ความคุ้มครองข้อมูลส่วนบุคคลที่เป็นหลักการทั่วไป จึงจำเป็นต้องตราพระราชบัญญัตินี้

<u>สาระสำคัญของ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒</u>

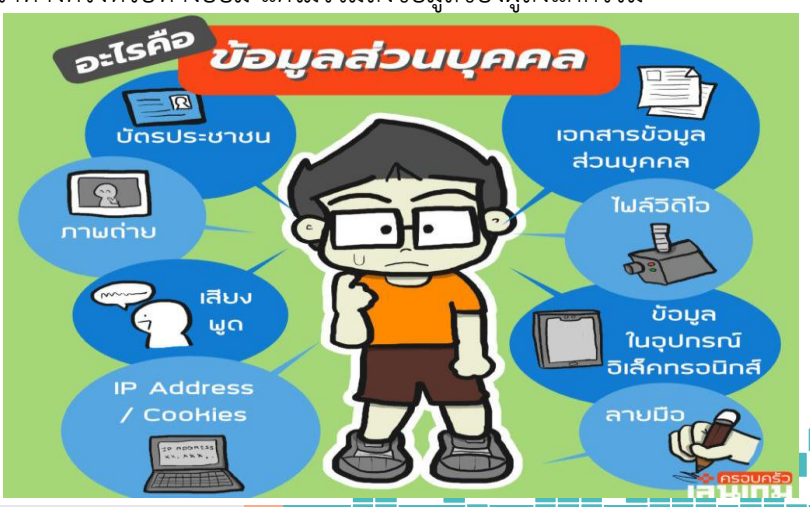
๑. เจ้าของข้อมูลต้องให้ความยินยอม (Consent) ในการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคลตามวัตถุประสงค์ที่ผู้เก็บรวบรวม ผู้ใช้ แจ้งไว้ตั้งแต่แรกเท่านั้น

๒. ผู้เก็บรวบรวมข้อมูลต้องรักษาความมั่นคงปลอดภัยของข้อมูล ไม่ให้มีการเปลี่ยนแปลงแก้ไข หรือถูกเข้าถึงโดยผู้ที่ไม่เกี่ยวข้องกับข้อมูล

๓. เจ้าของข้อมูลมีสิทธิถอนความยินยอม ขอให้ลบหรือทำลายข้อมูลเมื่อใดก็ได้ หากเป็นความประสงค์ของเจ้าของข้อมูล

<u>คำนิยาม</u>

ข้อมูลส่วนบุคคล (Personal Data) มาตรา ๖ ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรม



<u>สิทธิของเจ้าของข้อมูลส่วนบุคคล (Data Subject Right)</u>

๑. สิทธิได้รับการแจ้งให้ทราบ

๒. สิทธิเข้าถึงข้อมูลส่วนบุคคล

๓. สิทธิในการขอให้โอนข้อมูลส่วนบุคคล

๔. สิทธิคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล

๕. สิทธิขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลเป็นข้อมูลที่ไม่สามารถระบุตัวบุคคล

๖. สิทธิขอให้ระงับการใช้ข้อมูล

๗. สิทธิในการขอให้แก้ไขข้อมูลส่วนบุคคล

<u>ผู้เกี่ยวข้องกับข้อมูลส่วนบุคคล</u>

ผู้ควบคุมข้อมูลส่วนบุคคล (Data controller) บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่**ตัดสินใจ** เกี่ยวกับการเก็บ รวมรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล เพียงแค่เรามีการเก็บข้อมูลส่วนบุคคลของผู้อื่นไว้ ก็ถือว่าเราเป็นผู้ควบคุมข้อมูลส่วนบุคคล ที่จะต้องถือปฏิบัติตามกฎหมาย PDPA

ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor) บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล**ตามคำสั่งหรือในนาม**ของผู้ควบคุมข้อมูลส่วนบุคคล

เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer : DPO) บุคคลที่ได้รับการแต่งตั้งจากผู้ควบคุมข้อมูลส่วนบุคคล โดยที่จะต้องมีความรู้และความเข้าใจเกี่ยวกับกฎหมายข้อมูลส่วนบุคคลและประมวลผลข้อมูลองค์กร

<u>ข้อควรรู้เกี่ยวกับพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒</u>

๑. การเก็บข้อมูล ใช้ข้อมูล เปิดเผยข้อมูล ต้องได้รับความยินยอมเสมอ

๒. การขอความยินยอม ต้องทำเป็นหนังสือ หรือผ่านระบบออนไลน์ตามแบบที่กำหนดไว้

๓. การเก็บข้อมูล ต้องแจ้งรายละเอียดและแจ้งสิทธิต่อเจ้าของข้อมูล

๔. ต้องเก็บข้อมูลจากเจ้าของข้อมูลเท่านั้น ห้ามเก็บจากแหล่งอื่น

๕. ธุรกิจใหญ่ ต้องมีเจ้าหน้าที่คุ้มครองข้อมูลของตัวเอง

๖. การเก็บและให้ใช้ข้อมูล ถูกตรวจสอบโดยคณะกรรมการผู้เชี่ยวชาญ

๗. ข้อมูลคนตาย กฎหมายไม่คุ้มครอง

๘. คุ้มครองข้อมูลของคนในประเทศ ไม่ว่าบริษัทตั้งอยู่ที่ใด

๙. หากฝ่าฝืน กฎหมายนี้ อาจโดนค่าเสียหายเชิงลงโทษ จ่ายสองเท่า

<u>บุคคลทั่วไป พึงปฏิบัติ</u>

๑. ก่อนจะให้ข้อมูลสำคัญ ควรมีการเก็บบันทึกหลักฐานไว้

๒. การขอสำเนาของเอกสารที่มีข้อมูลส่วนบุคคล ควรมีการเก็บบันทึกหลักฐาน

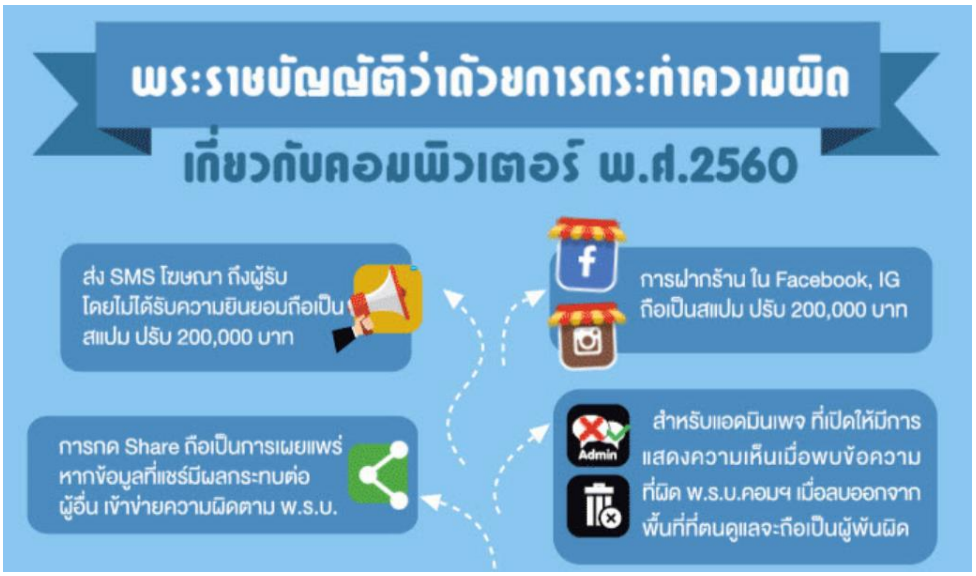
๓. มีสติรอบคอบในการให้ข้อมูลส่วนบุคคลแก่เว็บไซต์/แอปพลิเคชัน

๔. การโพสต์ข้อความหรือรูปภาพ ควรมีการตรวจสอบก่อน

๕. เจ้าของข้อมูลต้องทำหน้าที่ “คุ้มครองข้อมูลของตนเอง”

<u>พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐</u>

เหตุผลที่ประกาศใช้พระราชบัญญัตินี้ เนื่องจากพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ๒๕๕๐ มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน ซึ่งมีรูปแบบการการะทำความผิดที่มีความซับซ้อนมากขึ้นตามพัฒนาการทางเทคโนโลยีซึ่งเปลี่ยนแปลงอย่างรวดเร็ว สมควรปรับปรุงบทบัญญัติในส่วนที่เกี่ยวกับผู้รักษาการตามกฎหมาย กำหนดฐานความผิดใหม่ และแก้ไขเพิ่มเติมฐานความผิดเดิม รวมทั้งบทกำหนดโทษของความผิดดังกล่าว การปรับปรุงกระบวนการและหลักเกณฑ์ในการระงับการทำให้แพร่หลายหรือลบข้อมูลคอมพิวเตอร์ จึงจำเป็นต้องตราพระราชบัญญัตินี้



<u>ภัยคุกคาม และความเสี่ยง</u>

Phishing คือ การสร้างสถานการณ์โดยการส่งข้อความ E-mail หรือเว็บไซต์ปลอม เพื่อเป็นเหยื่อล่อให้ผู้ใช้งานเข้ามาติดเบ็ด และหลอกล่อผู้ใช้ให้กรอกข้อมูลส่วนตัวต่างๆ หรือส่งโปรแกรมให้ติดตั้งลงเครื่องคอมพิวเตอร์ตามที่แฮกเกอร์ต้องการ ซึ่งการทำ Phishing ที่พบเห็นในประเทศไทยมีอยู่ ๒ แบบคือ

๑. E-mail Phishing เป็นการส่ง E-mail หลอกลวงต่าง ๆ โดยอาจจะใช้ความสัมพันธ์ของบุคคล สถาบันการเงิน หรือตำแหน่ง เช่น CEO เจ้าของบริษัท หรือเจ้าหน้าที่ธนาคาร เพื่อให้ผู้ที่ได้รับ E-mail ไม่สงสัยและเชื่อถือ ซึ่งเนื้อหาใน E-mail นั้น อาจบอกถึงความจำเป็นเร่งด่วน ที่จะต้องกรอกข้อมูล หรือแจ้งการให้ข้อมูลส่วนบุคคล เช่น username และ password สำหรับเข้าระบบขององค์กร หรือจะเป็น username และ password สำหรับใช้ในการทำธุรกรรมทางการเงินอย่าง E-Banking เป็นต้น

๒. Web Phishing คือ การปลอมแปลงหน้าเว็บไซต์จริง เพื่อหลอกเอาข้อมูล เช่น username&password ของผู้ใช้งาน ถ้าหากผู้ใช้งานไม่ระมัดระวังก็อาจจะกรอกข้อมูลต่าง ๆ ส่งให้แฮกเกอร์โดยที่ไม่รู้ตัว โดย Web Phishing มักจะเป็นลิงก์ปลอมที่แนบมากับ E-mail เมื่อเหยื่อกดเปิดก็จะเข้าสู่ Web Phishing เว็บไซต์ปลอมที่ทำเลียนแบบเว็บไซต์ของจริงเพื่อหลอกให้เหยื่อกรอก username และ password หรือข้อมูลส่วนตัวอื่น ๆ ทันที โดยทั้งหมดทำผ่านหน้าเว็บที่คล้ายของจริง ที่แฮกเกอร์เป็นคนตั้งขึ้นมา เมื่อกรอกข้อมูลลงไป จึงส่งข้อมูลตรง ๆ ไปยังแฮกเกอร์

วิธีสังเกต E-mail หลอกลวง

๑. อย่าไว้ใจชื่อผู้ส่งที่แสดงใน E-mail

๒. ลองวางเมาส์ไปชี้ข้อความใน E-mail หากตัวอักษรไม่ตรงกับคำอธิบาย อย่ากดคลิก

๓. ตรวจสอบคำที่สะกดผิด

๔. พิจารณาถึงคำขึ้นต้นของ E-mail ว่าชัดเจนหรือไม่

๕. บริษัททั่ว ๆ ไป มักจะไม่ถามข้อมูลส่วนตัวใน E-mail

๖. ระวังไฟล์ที่แนบมาด้วย โดยชื่อของไฟล์จะยาวเป็นพิเศษ ไอคอนอาจจะเป็นของปลอม

Smishing หรือ SMS phishing คือการหลอกลวงทางข้อความ โดย scammers จะแอบอ้างตัวเองว่าเป็น บริษัทที่ถูกต้องตามกฎหมาย เพื่อพยายามขโมยข้อมูลส่วนตัวหรือข้อมูลทางการเงินของเหยื่อด้วยการส่ง notification ไปที่โทรศัพท์ของเหยื่อบ่อย ๆ

Smishing เป็นรูปแบบหนึ่งของ social engineering คือ เทคนิคการ Hacking ของ Hacker ซึ่งอาศัยช่องโหว่จากพฤติกรรมของผู้ใช้ ที่จะเล่นกับอารมณ์ความไว้วางใจ ความสับสน และความเร่งรีบในชีวิตของเหยื่อ เพื่อให้เหยื่อทำตามแผนของเหล่า scammers

วิธีป้องกัน SMS ดูดเงินโทรศัพท์

๑. ไม่โหลดแอปพลิเคชันเถื่อน

๒. ไม่โหลดแอปพลิเคชันที่ไม่จำเป็นต่อการใช้งาน

๓. หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่คุ้นเคย

๔. ก่อนกดยืนยันต่างๆ ควรตรวจสอบข้อมูลโดยละเอียด

๕. ตรวจสอบใบเสร็จค่าโทรศัพท์ทุกครั้งก่อนชำระค่าบริการ

Vishing Phishing คำว่า **Vishing** มาจากคำว่า **Voice Phishing** เป็นการ Phishing อีกรูปแบบหนึ่ง โดยแทนที่อาชญากรเลือกที่จะขอข้อมูลบัญชี รหัสผ่าน หรือข้อมูลธุรกรรมผ่านทางโทรศัพท์แทนที่จะใช้ E-mail โดยแฮกเกอร์ ซึ่งเมืองไทย คุ้นเคยคำว่า “แก๊งคอลเซ็นเตอร์”

วิธีรับมือกับแก๊งคอลเซ็นเตอร์

๑. ตั้งสติก่อนรับสายมิจฉาชีพชอบทำให้เราตกใจหรือกลัวจนรีบทำตามที่บอกต้องตั้งสติ

๒. วางสาย หากมั่นใจแล้วว่าเป็นมิจฉาชีพ เก็บหลักฐานและข้อมูลไว้แจ้งเบาะแส

๓. อย่าคุย หากสงสัยว่าเป็นมิจฉาชีพ ยิ่งคุยต่อจะยิ่งเพิ่มความเสี่ยง ให้รีบวางสาย

๔. อย่าบอกข้อมูลส่วนตัว เช่น ชื่อ นามสกุล เลขบัตรประชาชน วัน เดือน ปีเกิด แก่ผู้อื่น

๕. อย่าโอนเงิน ตามที่ปลายสายบอก มิจฉาชีพมักใช้กลลวง วนเข้าเรื่องเงินเสมอ

ประโยชน์ของการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

ปัจจุบันภัยคุกคามทางไซเบอร์ เกิดขึ้นเป็นจำนวนมาก ในหลายๆ เหตุการณ์ก็มีความเกี่ยวเนื่องกับทุกคนในชีวิตประจำวัน ซึ่งถือเป็นความเสี่ยงอย่างมากที่จะก่อให้เกิดความเสียหายต่อทั้งตัวเรา ทรัพย์สิน และต่อองค์กรที่เราทำงานอยู่ เนื่องจากมิจฉาชีพเข้ามาในหลากหลายรูปแบบ เราจึงควรหาแนวทางป้องกันภัยทางไซเบอร์ โดยการเรียนรู้ถึงแนวทางป้องกันภัยที่อาจจะเกิดขึ้น และกฎหมายที่คุ้มครองข้อมูลส่วนบุคคล เพื่อจะได้รู้แนวทางปฏิบัติ หากเกิดภัยด้านเทคโนโลยีสารสนเทศ โดยประชาชนทั่วไปสามารถขอให้ลบ ทำลาย หรือขอให้ระงับการใช้ ข้อมูลส่วนบุคคลได้ สามารถร้องเรียนและขอให้ผู้ละเมิดชดใช้ค่าสินไหมทดแทน หากมีการใช้ข้อมูลนอกเหนือจากวัตถุประสงค์ที่แจ้งมา เพื่อลดความเดือดร้อนรำคาญ หรือความเสียหายอันเกิดจากการละเมิดข้อมูลส่วนบุคคล

จัดทำโดย
นางสาวพนิตนาฏ หิตโกเมท
ตำแหน่ง นักทรัพยากรบุคคลปฏิบัติการ
กลุ่มพัฒนาระบบงานและอัตรากำลัง กองการเจ้าหน้าที่
๒๑ กุมภาพันธ์ ๒๕๖๖