สรุปบทเรียนการพัฒนาความรู้

หลักสูตร

โครงการเสริมสร้างความรู้ความเข้าใจ และสร้างความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

****

ชื่อ-สกุล (ภาษาไทย) นางสาวอลีนา รัตนไพโรจน์ **ตำแหน่ง** นักวิทยาศาสตร์ปฏิบัติการ

สังกัด กลุ่มวิจัยสิ่งแวดล้อมดิน

วันที่อบรม 18 พฤษภาคม พ.ศ.2566

วัตถุประสงค์ของหลักสูตร

1. เพื่อให้เกิดความตระหนักถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน แนวทางการป้องกัน และแก้ไข
2. เพื่อให้เกิดความรู้เกี่ยวกับกฎหมายและมาตรการรักษาความปลอดภัยไซเบอร์

สรุปบทเรียน

คำนิยาม

ไซเบอร์ (Cyber) หมายความว่า ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบบอินเตอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการปกติของดาวเทียม และระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง และเป็นภัยอันตรายที่ก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

การรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

อันดับ ภัยไซเบอร์ใกล้ตัวที่คนไทยถูกหลอกมากที่สุด

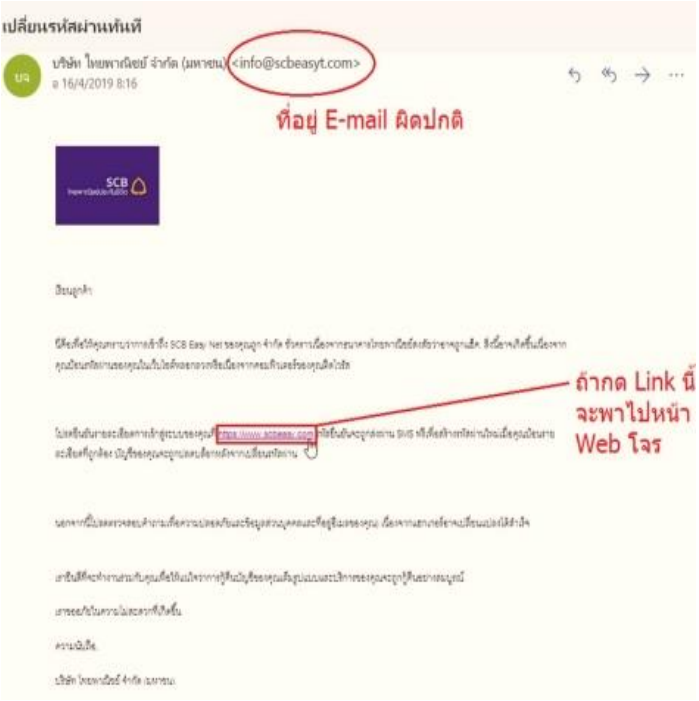
<u>ภัยประเภทที่ 1 มิจฉาชีพบนโซเชียลมีเดียและการโจมตีแบบ Social Engineering</u>

การโจมตีแบบ Social Engineering คือ การหลอกใช้จุดอ่อนของมนุษย์จากความกลัว ความเร่งรีบ ความโลภ ความอยากรู้อยากเห็น การสร้างความน่าเชื่อถือ การเบี่ยงเบนความสนใจ เพื่อขโมยข้อมูลหรือหลอกล่อให้เหยื่อกระทำบางสิ่งบางอย่างตามที่ผู้ประสงค์ร้ายมุ่งหวัง ตัวอย่างการโจมตีด้วยวิธีนี้ เช่น การส่งอีเมลหลอกให้ผู้ใช้เข้าไปยังเว็ปไซต์ปลอมเพื่อขโมยรหัสผ่านหรือการโทรศัพท์หลอกเหยื่อว่าได้รับรางวัลแต่ต้องโอนเงินค่าดำเนินการก่อน

วิธีรับมือและป้องกัน อย่าหลงเชื่อข้อความผ่านแชท เพื่อขอให้โอนเงินหรือขอข้อมูลใด ๆ หากผู้ส่งข้อความเป็นเพื่อนควรติดต่อเพื่อนโดยตรงผ่านช่องทางอื่นเพื่อยืนยันตัวตนและจุดประสงค์ก่อน

ภัยประเภทที่ 2 อีเมลหลอกลวง (Phishing)

ฟิชชิงเป็นหนึ่งในการหลอกลวงทางโลกออนไลน์ที่พบได้บ่อยที่สุด ฟิชชิงมีหลายรูปแบบ การหลอกลวงประเภทนี้มักจะเกี่ยวข้องกับการใช้กลอุบายหลอกล่อผู้ใช้งาน และการแอบอ้างเป็นเว็ปไซต์ที่น่าเชื่อถือ เช่น เว็ปไซต์ธนาคาร หรือบัญชีโซเชียลมีเดีย ซึ่งมักจะแตกต่างจากของจริง มีการเปลี่ยนชื่อในลิงค์เพียงเล็กน้อยทำให้เราไม่สังเกต ฟิชชิงประเภทต่างๆ ได้แก่ สเปียร์ฟิชชิง (Spear phishing) วาฬลิง (Whaling) ฟาร์มมิง (Pharming)



ตัวอย่างอีเมลหลอกลวง

วิธีรับมือและป้องกัน หากได้รับอีเมลต้องสงสัยให้ “คิด” ก่อน “คลิก” ควรตรวจสอบผู้ส่ง เนื้อหาและลิงค์ภายในโดยละเอียด ก่อนตอบกลับหรือให้ข้อมูลใด ๆ ทุกครั้ง

ภัยประเภทที่ 3 การขโมยข้อมูลส่วนบุคคล (Data Theft) มีหลายรูปแบบได้แก่

3.1 การหลอกลวงทางอินเตอร์เน็ต (Scam) เช่น สแกมบัตรเครดิต โรแมนซ์สแกม

3.2 มัลแวร์ (Malware) หรือ Mulicious Code เป็นโปรแกรมที่ถูกพัฒนาขึ้นเพื่อให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ เช่น ทำให้เกิดความขัดข้อง หรือเสียหายกับระบบที่โปรแกรมดังกล่าวติดตั้งอยู่ โดยปกติภัยคุกคามประเภทนี้ ต้องอาศัยการหลอกลวงผู้ใช้งานเรียกใช้งานโปรแกรมก่อนจึงจะสามารถทำการโจมตีได้ เช่น Virus Trojan Spyware หรือบางครั้งอาจทำการโจมตีได้ด้วยตนเอง เช่น Worm

3.3 แรนซัมแวร์ (Ransomware) หรือมัลแวร์เรียกค่าไถ่ จะเกิดเหตุขึ้นเมื่อเปิดไฟล์แนบ รวมถึงเอกสารที่แชร์ผ่านเครือข่ายและจากอุปกรณ์ External Drive ที่เสียบอยู่กับเครื่องคอมพิวเตอร์ ซึ่งไฟล์ของ

เครื่องเหยื่อจะยังอยู่ แต่ไม่สามารถเปิดอ่านข้อมูลได้ จนกว่าจะจ่ายเงินเพื่อเป็นค่าใช้จ่ายในการส่งรหัสสำหรับถอดรหัสลับข้อมูล (Decryption) กลับมา

วิธีรับมือและป้องกัน 1. สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอและหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ

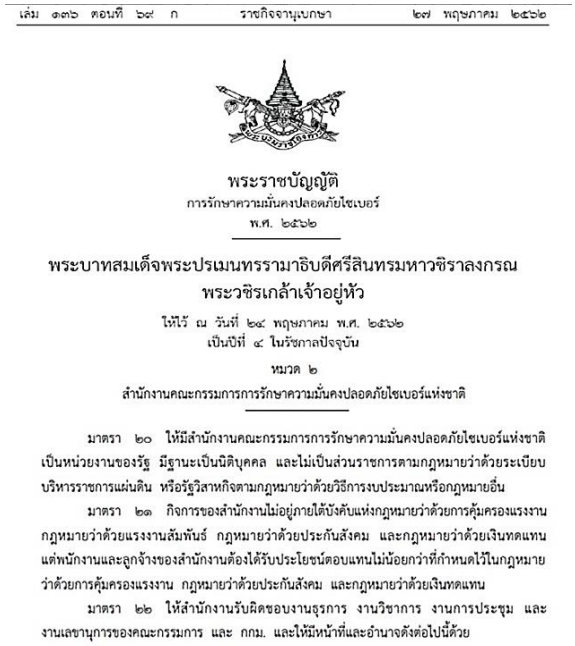
2. อัปเดตโปรแกรมแอนติไวรัส รวมถึงโปรแกรมอื่น โดยเฉพาะโปรแกรมที่มักมีปัญหาเรื่องช่องโหว่

3. ไม่คลิกลิงค์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัย หากไม่มั่นใจว่าเป็นอีเมลที่น่าเชื่อถือหรือไม่เคยรู้จักมาก่อน

4. ดาวน์โหลดซอฟแวร์ที่น่าเชื่อถือเท่านั้น เพราะผู้ร้ายอาจฝังมัลแวร์ในซอฟแวร์ที่เปิดดาวน์โหลดฟรี

กฎหมายที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

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



เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

หมวด ๒
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๒๐ ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

มาตรา ๒๑ กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

มาตรา ๒๒ ให้สำนักงานรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการ และ กกม. และให้มีหน้าที่และอำนาจดังต่อไปนี้ด้วย

มีผลบังคับใช้เมื่อ 25 พฤษภาคม พ.ศ. 2562 เจตนารมณ์ของพระราชบัญญัติฉบับนี้ เพื่อให้มีมาตรการในการ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เช่น ไวรัส มัลแวร์ อาชญากรคอมพิวเตอร์ ที่ทำให้ระบบคอมพิวเตอร์หรือโครงข่ายของหน่วยงานโครงสร้างพื้นฐานที่สำคัญไม่สามารถทำงานได้เป็นปกติกระทบต่อการให้บริการแก่ประชาชน หรือความสงบเรียบร้อยภายในประเทศ

ประโยชน์ที่ได้รับต่อตนเอง

ช่วยลดความเสี่ยงจากการโจมตีทางไซเบอร์ และพร้อมรับมือต่อภัยคุกคามทุกรูปแบบอย่างทันท่วงที

ประโยชน์ที่ได้รับต่อหน่วยงาน

ใช้เป็นมาตรการหรือแนวทางปฏิบัติในการป้องกันความเสี่ยงจากภัยคุกคามไซเบอร์อันกระทบต่อความมั่นคงของรัฐ และพร้อมตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ