สรุปรายงานการประชุม
ส่งเสริมและสนับสนุนทักษะความเข้าใจและใช้เทคโนโลยีดิจิทัลของกรมอนามัย (Digital Literacy) ครั้งที่ ๒/๒๕๖๖
เรื่อง การสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness)
วันที่ ๒๗ พฤศจิกายน ๒๕๖๖ เวลา ๐๙.๓๐ - ๑๖.๓๐ น.
ณ ห้องประชุมกองแผนงาน อาคาร ๕ ชั้น ๔ กรมอนามัย

รายชื่อผู้เข้าร่วมประชุม

๑.	นายอาณัตชัย จันทร์ต่าย	เจ้าหน้าที่คอมพิวเตอร์	สำนักงานเลขานุการกรม
๒.	นางสาวพัทธนันท์ วังเสนา	นักวิชาการพัสดุ	ศูนย์ความร่วมมือระหว่างประเทศ
๓.	นางสาวจิราภรณ์ สุ่มติ๊บ	นักวิชาการคอมพิวเตอร์	ศูนย์ความร่วมมือระหว่างประเทศ
๔.	นางสาวจิรฐา คุ้มทอง	นักวิชาการพัสดุ	กลุ่มตรวจสอบภายใน
๕.	นายณัฐวิทย์ ญาดี	นักวิชาการคอมพิวเตอร์	กองส่งเสริมความรอบรู้และสื่อสารสุขภาพ
๖.	นางสาวกาญจนรินทร์ มหาวี	นักวิเคราะห์นโยบายและแผน	กองส่งเสริมความรอบรู้และสื่อสารสุขภาพ
๗.	นางสาววริษา วงศ์วาณิชวัฒนา	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	สำนักโภชนาการ
๘.	นางสาววรินดา ดาอ่ำ	นักโภชนาการ	สำนักโภชนาการ
๙.	นายจักรพันธุ์ บุญชู	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	สำนักโภชนาการ
๑๐.	นายปฏิวัติ เหลืองสถิตย์	นักเทคโนโลยีสารสนเทศ	สำนักอนามัยผู้สูงอายุ
๑๑.	นายนันทวัฒน์ จองคำ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กองการเจ้าหน้าที่
๑๒.	นายอภัย ปิณฑะคุปต์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กองประเมินผลกระทบต่อสุขภาพ
๑๓.	นายสันสนะ ณรงค์อินทร์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กองกิจกรรมทางกายเพื่อสุขภาพ
๑๔.	นายรังสฤษดิ์ เชื้อดวงผุย	นักวิชากานพัสดุปฏิบัติการ	กองคลัง
๑๕.	นางสาวลดาวัลย์ จิตขาว	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	สำนักอนามัยการเจริญพันธุ์
๑๖.	นางสาวอารีรัตน์ อาลากุล	นักวิชาการคอมพิวเตอร์	กองนวัตบริการสุขภาวะ
๑๗.	นายสุเมธา บุญประเสริฐ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	สำนักสุขาภิบาลอาหารและน้ำ
๑๘.	นางสาวอรุณิญา โชคลาภ	นักวิชาการสาธารณสุขปฏิบัติการ	สำนักสุขาภิบาลอาหารและน้ำ
๑๙.	นายวนนท์ บากี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	สำนักอนามัยสิ่งแวดล้อม
๒๐.	นายจันท์จิรา สวารักษ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	สำนักอนามัยสิ่งแวดล้อม
๒๑.	นายศุภชัย เครือเมฆ	เจ้าพนักงานธุรการจัดงานทั่วไป	กองกฎหมาย
๒๒.	นายไอลวิล ขันธสนธิ์	นักวิชาการคอมพิวเตอร์	กองกฎหมาย
๒๓.	นายประดิภาส สุขเสาร์เกิด	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ศูนย์อนามัยที่ ๕ ราชบุรี
๒๔.	นายจักรพันธ์ สุขใส	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ศูนย์อนามัยที่ ๗ ขอนแก่น
๒๕.	นางสาวรุ้งลาวัลย์ ตรงกะพงศ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ศูนย์อนามัยที่ ๘ อุดรธานี
๒๖.	นายอิมรอน บินอาแว	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ศูนย์อนามัยที่ ๑๒ ยะลา
๒๗.	นายสุรสีห์ ฉันทกุล	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	ศูนย์อนามัยกลุ่มชาติพันธุ์ ชายขอบ และแรงงานข้ามชาติ

เริ่มประชุมเวลา ๐๙.๓๐ น.

วาระที่ ๑ เรื่องที่ประธานแจ้งให้ทราบ

-

วาระที่ ๒ เรื่องเพื่อทราบ

แนวโน้มภัยคุกคามในปัจจุบัน ผู้โจมตีทางไซเบอร์หรือแฮกเกอร์ (Hacker) ใช้วิธีที่ซับซ้อนขึ้น เน้นสร้างความเสียหายทางเศรษฐกิจ หรือที่ส่งผลต่อความมั่นคงของชาติ โดยมีหลายรูปแบบด้วยกัน เช่น

๑. Sniffing คือ การดักจับข้อมูลที่มีการรับ-ส่งบนระบบเครือข่าย วิธีป้องกันคือ ไม่ควรใช้ระบบเครือข่ายฟรีทั่วไป (Free Wi-Fi) ในการทำกิจกรรมที่สำคัญ เช่น ธุรกรรมการเงิน เป็นต้น

๒. Spam คือ การส่งข้อความที่ผู้รับไม่ได้ร้องขอเป็นโฆษณาชวนเชื่อต่าง ๆ เช่น ทาง E-mail เป็นต้น

๓. Phishing คือ การหลอกลวงทางอินเทอร์เน็ต เช่น หลอกให้กดลิงก์ปลอม เพื่อให้กรอกข้อมูลที่สำคัญลงไป แล้วนำไปใช้ในทางที่ผิด

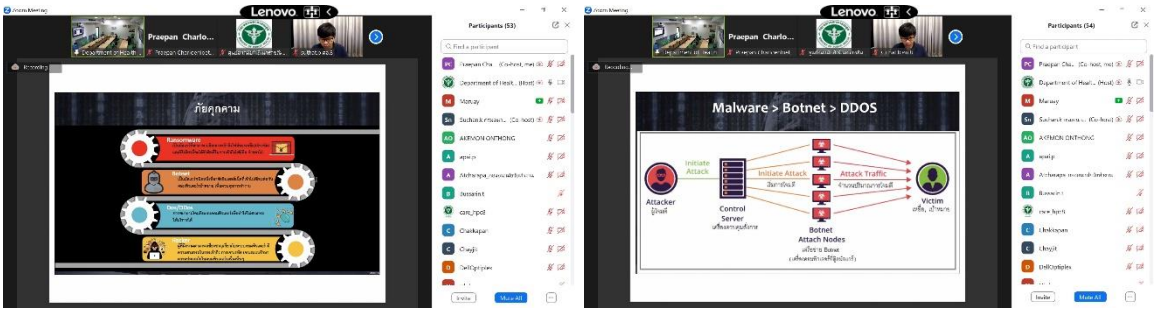
๔. Social Engineering คือ การใช้จิตวิทยาในการหลอกลวง เพื่อให้เปิดเผยข้อมูลที่เป็นความลับ

๕. Ransomware คือ มัลแวร์ที่สามารถบล็อกการเข้าถึงไฟล์บนเครื่องคอมพิวเตอร์/อุปกรณ์ของเหยื่อ เพื่อเรียกค่าไถ่ จึงจะได้รับการปลดบล็อกแล้วเข้าถึงไฟล์ได้อีกครั้ง

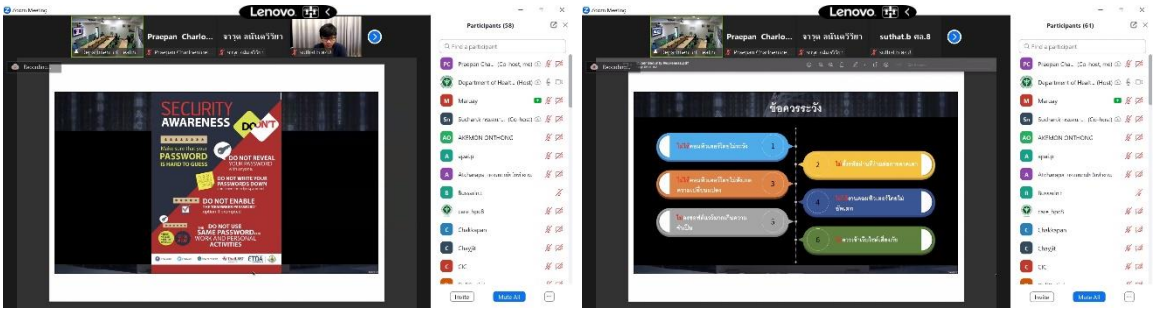
๖. Botnet คือ มัลแวร์ที่อาศัยอินเทอร์เน็ตที่เข้าไปเชื่อมกับคอมพิวเตอร์เหยื่อ เพื่อควบคุมการทำงาน

๗. Dos/DDos คือ การพยายามโจมตีระบบเครือข่ายคอมพิวเตอร์ เพื่อทำให้ไม่สามารถให้บริการนั้นได้

๘. Hacker คือ คนที่มีความรู้ ความเชี่ยวชาญเกี่ยวกับระบบเครือข่ายคอมพิวเตอร์ หรือระบบความปลอดภัย เพื่อเข้าถึงข้อมูล หรือกระทำความผิดต่าง ๆ



- รูปแบบการโจมตี เช่น การผสมผสานระหว่าง มัลแวร์, Botnet และ DDos มีลักษณะคือ ผู้โจมตีจะมีเครื่องควบคุมสั่งการ เช่น เซิฟเวอร์หรือแล็บท็อป โดยจะเขียนไวรัส (มัลแวร์) ส่งไปที่เครื่องคอมพิวเตอร์ของเหยื่อและแพร่กระจายอยู่ในเครือข่ายหรือองค์กรนั้น ๆ ฝังตัวเป็น Botnet โดยไม่รู้ตัว จนกระทั่งผู้โจมตีสั่งการไปที่เครื่องทั้งหมดเหล่านั้น เพื่อสั่งโจมตีเป้าหมายด้วยจำนวนที่มาก ที่จะทำให้ระบบ ๆ หนึ่งไม่สามารถให้บริการได้ (DDos)



- การตั้งรหัสผ่านที่ปลอดภัย เพื่อให้ผู้โจมตีคาดเดาได้ยาก เช่น มีส่วนประกอบของตัวพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข อักษรพิเศษ และไม่ใช้คำที่อยู่บนพจนานุกรม หรือคำศัพท์ที่ใกล้ตัว และควรตั้งรหัสผ่านสำหรับใช้งานส่วนตัวกับใช้ที่ทำงานให้แตกต่างกัน

- สรุปข้อควรระวัง เช่น

๑. ไม่ใช้คอมพิวเตอร์โดยไม่ระวัง เช่น ไม่ใช้คอมพิวเตอร์ที่ทำงานในการส่วนตัว
๒. ไม่ตั้งรหัสผ่านที่ง่ายต่อการคาดเดา
๓. ไม่ใช้คอมพิวเตอร์โดยไม่สังเกตความเปลี่ยนแปลง เช่น มีไฟล์ไม่คุ้นบนเครื่องหรือไม่
๔. ไม่ใช้งานคอมพิวเตอร์หรืออุปกรณ์มือถือ โดยไม่อัปเดตให้เป็นเวอร์ชันปัจจุบัน
๕. ไม่ลงซอฟต์แวร์มากเกินความจำเป็น
๖. ไม่ควรเข้าเว็บไซต์เสี่ยงภัย
๗. ไม่ปฏิบัตินอกเหนือกฎหมายเกี่ยวกับการใช้งานอินเทอร์เน็ต
๘. ไม่หลงเชื่อโดยง่าย
๙. ไม่ทำธุรกรรมออนไลน์โดยไม่สังเกตสัญลักษณ์ความปลอดภัย
๑๐. ไม่เปิดเผยข้อมูลส่วนตัวลงบนโซเชียลมีเดีย
๑๑. ไม่มีอะไรได้มาฟรี
๑๒. ไม่ตื่นตระหนัก
๑๓. รหัสผ่านควรเป็นความลับ เช่น ไม่เขียนรหัสแปะไว้ที่หน้าจอคอมฯ
๑๔. ไม่หลงผิดไปกับสิ่งผิดกฎหมาย
๑๕. เสพสื่ออย่างมีวิจารณญาณ
๑๖. โพสต์สิ่งใดให้ทำด้วยความระมัดระวัง
๑๗. แชร์ต่ออย่างมีสติ
๑๘. รู้เท่าทันสื่อสังคมออนไลน์

โดยเมื่อพบหรือคาดว่าจะถูกโจมตี ให้รีบดำเนินการถอดสายแลนหรือยกเลิกการเชื่อมต่ออินเทอร์เน็ตทันที เพื่อไม่ให้ไวรัสแพร่กระจายไปยังเครื่องอื่น ๆ แล้วรีบแจ้งเจ้าหน้าที่ IT โดยด่วน

พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ คือ กฎหมายที่ตราขึ้นเพื่อให้ประเทศไทยมีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ที่กระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ มีการประสานความร่วมมือระหว่างผู้เกี่ยวข้อง พัฒนาความรู้ ความสามารถของของบุคลากรและผู้เชี่ยวชาญ รวมถึงการให้ความรู้และความตระหนักถึงภัยไซเบอร์

- ไซเบอร์ หมายความรวมถึง ข้อมูลและการสื่อสาร ที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม

- ภัยคุกคามทางไซเบอร์ หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

- การรับมือภัยคุกคามทางไซเบอร์ มีการแบ่งระดับของภัยคุกคาม ไว้ดังนี้

๑. ระดับไม่ร้ายแรง: ภัยคุกคามทางไซเบอร์ ที่มีความเสี่ยงทำให้ระบบคอมพิวเตอร์หรือการให้บริการด้วยประสิทธิภาพลง

๒. ระดับร้ายแรง: ภัยคุกคามทางไซเบอร์ ที่มีจุดมุ่งหมายในการโจมตีโครงสร้างพื้นฐานสำคัญของประเทศให้เสียหาย จนไม่สามารถทำงานหรือให้บริการได้

๓. ระดับวิกฤต: ภัยคุกคามทางไซเบอร์ ที่มีระดับสูงกว่าระดับร้ายแรง ทำให้โครงสร้างพื้นฐานล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ได้ และอาจส่งผลต่อสวัสดิภาพของประชาชน กระทบต่อความสงบเรียบร้อย ทำให้ประเทศตกอยู่ในภาวะคับขัน

- แนวทางในการรับมือภัยคุกคามทางไซเบอร์

๑. People: มีการจัดอบรมสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับพนักงาน (Cybersecurity Awareness) และมีการทดสอบ

๒. Process: ตรวจสอบและรายงานผลการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน หรือปฏิบัติตามมาตรฐานสากล

๓. Technology: มีการดำเนินการตรวจสอบช่องโหว่และทดสอบเจาะระบบ (Vulnerability Assessment/Penetration Testing) หรือจัดการทดสอบรับมือภัยคุกคามไซเบอร์

พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มีสาระสำคัญ ดังนี้

๑. ผู้เก็บข้อมูลต้องชี้แจงข้อมูลที่จะเก็บรวบรวม และต้องได้รับอนุญาตหรือความยินยอมจากเจ้าของข้อมูลเท่านั้น จึงจะสามารถใช้และเข้าถึงข้อมูลของเจ้าของข้อมูลได้

๒. ผู้เก็บรวบรวมข้อมูลจะต้องรักษาข้อมูลให้เป็นความลับ

๓. เจ้าของข้อมูลสามารถยกเลิกสิทธิ์การเข้าถึงข้อมูลของผู้เก็บข้อมูล ลบ หรือทำลายได้

- สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (ส.ค.ส.) เป็นหน่วยงานที่คอยกำหนดมาตรฐานในการเก็บรวบรวม การใช้ การเปิดเผยข้อมูลส่วนบุคคล และให้ความรู้แก่เจ้าหน้าที่ภาครัฐ เอกชน และบุคคลทั่วไป

- คณะกรรมการผู้เชี่ยวชาญ มีหน้าที่ พิจารณาเรื่องร้องเรียนเมื่อมีการละเมิด ตรวจสอบผู้เก็บข้อมูลส่วนบุคคล หรือผู้ประมวลผลข้อมูล ที่ก่อให้เกิดความเสียหายแก่เจ้าของข้อมูลส่วนบุคคล

- บทลงโทษ หากผู้เก็บรวบรวมข้อมูลฝ่าฝืน ได้แก่

๑. โทษทางอาญา จำคุกไม่เกิน ๖ เดือนถึง ๑ ปีหรือปรับไม่เกิน ๕ แสนถึง ๑ ล้านบาท

๒. โทษทางปกครอง ปรับไม่เกิน ๕ แสนบาท ถึง ๕ ล้านบาท

พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ เป็นกฎหมายที่ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อป้องกัน และควบคุมการกระทำผิดที่จะเกิดขึ้นจากการใช้คอมพิวเตอร์ได้ มีบทลงโทษ เช่น

๑. เข้าถึงระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต จำคุกไม่เกิน ๖ เดือน ปรับไม่เกิน ๑ หมื่นบาท

๒. เข้าถึงข้อมูลคอมพิวเตอร์โดยไม่ได้รับอนุญาต จำคุกไม่เกิน ๒ เดือน ปรับไม่เกิน ๔ หมื่นบาท

๓. นำมาตรการป้องกันระบบไปเผยแพร่ จำคุกไม่เกิน ๑ ปี ปรับไม่เกิน ๒ หมื่นบาท

๔. ดักรับข้อมูลคอมพิวเตอร์ จำคุกไม่เกิน ๒ ปี ปรับไม่เกิน ๔ หมื่นบาท หรือทั้งจำทั้งปรับ

๕. ขัดขวาง ทำร้ายระบบ ดัดแปลง หรือทำลายข้อมูลผู้อื่นเสียหาย จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑ แสนบาท หรือทั้งจำทั้งปรับ

๖. ส่งอีเมลขายของโดยที่ลูกค้าไม่ยินดีที่จะรับ ถือเป็น Spam จำคุกไม่เกิน ๒ ปี ปรับไม่เกิน ๑ แสนบาท หรือทั้งจำทั้งปรับ

๗. โพสต์ข่าวปลอม การก่อการร้าย ข้อมูลลามก โดยส่งผลกระทบต่อประชาชน จำคุกไม่เกิน ๕ ปี ปรับไม่เกิน ๑ แสนบาท หรือทั้งจำทั้งปรับ ส่วนที่ส่งผลต่อตัวบุคคลใดบุคคลหนึ่ง จำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๖ แสนบาท หรือทั้งจำทั้งปรับ

๘. การตัดต่อ ดัดแปลงภาพ ที่ทำให้ผู้อื่นเสียหาย และเสื่อมเสียชื่อเสียง รวมทั้งการโพสต์ภาพผู้เสียชีวิตที่ทำให้พ่อ, แม่, คู่สมรส หรือบุตรผู้ตายเสียชื่อเสียง หรือได้รับความอับอาย จำคุกไม่เกิน ๓ ปี ปรับไม่เกิน ๒ แสนบาท

วาระที่ ๓ เรื่องเพื่อพิจารณา

-

วาระที่ ๔ เรื่องอื่นๆ

-

จบประชุมเวลา ๑๖.๓๐ น.

จดบันทึกการประชุม
นายภัทร์รพี สีบุตตะ
นักวิชาการคอมพิวเตอร์
กองดิจิทัลเพื่อส่งเสริมสุขภาพ กรมอนามัย