ที่ นฐ ๐๐๓๓/๒๔๗๓

สำนักงานสาธารณสุขจังหวัดนครปฐม
๑๗๐ ถนนเทศา ตำบลพระปฐมเจดีย์
อำเภอเมือง จังหวัดนครปฐม ๗๓๐๐๐

๓๑ มกราคม ๒๕๖๖

เรื่อง แจ้งมาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์

เรียน ผู้อำนวยการโรงพยาบาลนครปฐม ผู้อำนวยการโรงพยาบาลชุมชนทุกแห่ง สาธารณสุขอำเภอทุกอำเภอ

สิ่งที่ส่งมาด้วย สำเนาหนังสือสำนักงานปลัดกระทรวงสาธารณสุข ที่ สธ ๐๐๒๑๒/ว ๑๙๐๘
ลงวันที่ ๒๖ มกราคม ๒๕๖๖ จำนวน ๑ ฉบับ

ตามที่สำนักงานปลัดกระทรวงสาธารณสุขโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Health CERT) ได้จัดประชุมชี้แจงแนวทางการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์เมื่อวันที่ ๑๘ มกราคม ๒๕๖๖ เพื่อแจ้งมาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์ของกระทรวงสาธารณสุข ๓ มาตรการได้แก่ มาตรการระดับประเทศ มาตราการจากส่วนกลาง และมาตรการเชิงพื้นที่ นั้น

ในการนี้เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงสาธารณสุขมีประสิทธิภาพและเห็นผลอย่างเป็นรูปธรรม สำนักงานสาธารณสุขจังหวัดนครปฐม ขอเน้นย้ำให้ทุกหน่วยงานในสังกัดสำนักงานสาธารณสุขจังหวัดนครปฐม ดำเนินการตามมาตรการเชิงพื้นที่ ทั้ง ๕ ประเด็น รายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อพิจารณาดำเนินการดังกล่าวอย่างเคร่งครัด

ขอแสดงความนับถือ

สุภัทร

(นายสุภัทร กตัญญูทิตา)
นักวิชาการสาธารณสุขชำนาญการพิเศษ (ด้านบริการทางวิชาการ) ปฏิบัติราชการแทน
นายแพทย์สาธารณสุขจังหวัดนครปฐม

กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข
โทร ๐ ๓๔๒๑ ๓๒๗๙ ๘๐ ต่อ ๒๒๓
โทรสาร ๐ ๓๔๒๕ ๑๕๕๐

ที่ สธ ๐๒๑๒/ว ๑๙๐๔

สำนักงานปลัดกระทรวงสาธารณสุข
ถนนติวานนท์ จังหวัดนนทบุรี ๑๑๐๐๐

๒๖ มกราคม ๒๕๖๖

เรื่อง มาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์

เรียน เลขาธิการคณะกรรมการอาหารและยา/อธิบดีกรมทุกกรม/นายแพทย์สาธารณสุขจังหวัดทุกแห่ง/ผู้อำนวยการสำนักงานเขตสุขภาพที่ ๑ – ๑๓/ผู้อำนวยการโรงพยาบาลศูนย์/ทั่วไป ทุกแห่ง หัวหน้าสำนักงานรัฐมนตรี และผู้อำนวยการหน่วยงานในสังกัดสำนักงานปลัดกระทรวงสาธารณสุข

สิ่งที่ส่งมาด้วย มาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์ จำนวน ๑ ชุด

ตามที่สำนักงานปลัดกระทรวงสาธารณสุขโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Health CERT) ได้จัดประชุมชี้แจงแนวทางการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์ เมื่อวันที่ ๑๘ มกราคม ๒๕๖๖ ณ ห้องประชุม Focus อาคาร ๒ ชั้น ๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข และผ่านสื่ออิเล็กทรอนิกส์ด้วยโปรแกรม Cisco WebEx Meeting เพื่อแจ้งมาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์ของกระทรวงสาธารณสุข ๓ มาตรการ ได้แก่ มาตรการระดับประเทศ มาตราการจากส่วนกลาง และมาตรการเชิงพื้นที่ นั้น

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Health CERT) จึงขอเน้นย้ำให้ทุกหน่วยงานดำเนินการตามมาตรการเชิงพื้นที่ทั้ง ๕ ประเด็น ประกอบด้วย ๑) สำรวจเว็บไซต์ของหน่วยงานทั้งหมด และจัดส่งให้ Health CERT ภายในวันที่ ๒๘ กุมภาพันธ์ ๒๕๖๖ ๒) ปิดเว็บไซต์ที่ไม่ได้ใช้งานและเว็บไซต์ที่มีความเสี่ยงทั้งหมด ๓) ดูแล Environments ทั้งหมดที่เกี่ยวข้อง ของเว็บไซต์ และอัปเดตให้ทันสมัย ๔) จัดหาอุปกรณ์ป้องกัน เช่น Firewall, Web Application Firewall และ Antivirus เป็นต้น และ ๕) เฝ้าระวังภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงสาธารณสุขมีประสิทธิภาพและเห็นผลอย่างเป็นรูปธรรม รายละเอียดตามสิ่งที่ส่งมาด้วย

จึงเรียนมาเพื่อโปรดทราบและมอบหมายหน่วยงานที่เกี่ยวข้องดำเนินการตามมาตรการโดยเคร่งครัดต่อไปด้วย จะเป็นพระคุณ

ขอแสดงความนับถือ

(นายพงศ์เกษม ไข่มุกด์)
รองปลัดกระทรวงสาธารณสุข
ปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
ประจำกระทรวงสาธารณสุข

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
โทร. ๐ ๒๕๙๐ ๑๒๑๓
ไปรษณีย์อิเล็กทรอนิกส์ ict-moph@health.moph.go.th

มาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กรณีการแฝงเว็บไซต์พนันออนไลน์)

กระทรวงสาธารณสุข

ตามที่สำนักงานปลัดกระทรวงสาธารณสุขโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Health CERT) ได้จัดประชุมชี้แจงแนวทางการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์ เมื่อวันที่ ๑๘ มกราคม ๒๕๖๖ ณ ห้องประชุม Focus อาคาร ๒ ชั้น ๑ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข และผ่านสื่ออิเล็กทรอนิกส์ด้วยโปรแกรม Cisco WebEx Meeting เพื่อแจ้งมาตรการการรักษาความมั่นคงปลอดภัยจากการแฝงเว็บไซต์พนันออนไลน์ของกระทรวงสาธารณสุข ๓ มาตรการ ได้แก่ มาตรการระดับประเทศ มาตราการจากส่วนกลาง และมาตรการเชิงพื้นที่ นั้น

ในการนี้ เพื่อให้หน่วยงานในสังกัดกระทรวงสาธารณสุขสามารถดำเนินการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้อย่างมีประสิทธิภาพและเห็นผลอย่างเป็นรูปธรรม กระทรวงสาธารณสุขจึงได้กำหนดมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กรณีการแฝงเว็บไซต์พนันออนไลน์) กระทรวงสาธารณสุข ไว้ดังต่อไปนี้

๑. มาตการระดับประเทศ

กระทรวงสาธารณสุขพร้อมให้ความร่วมมือกับ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และหน่วยงานที่เกี่ยวข้อง รวมถึงให้การสนับสนุนนโยบายในระดับประเทศ ในการแก้ไขปัญหาด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. มาตการจากส่วนกลาง

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ (Health CERT) ดำเนินการ ดังนี้

๑) จัดทำทะเบียนเว็บไซต์

๒) สนับสนุนการปิดโดเมนที่เป็นอันตราย หาก Health CERT ตรวจสอบพบเว็บไซต์ที่ถูกคุกคามทางไซเบอร์แล้วหน่วยงานไม่สามารถดำเนินการแก้ไขได้ภายใน ๒๔ ชั่วโมง Health CERT จะดำเนินการปิดโดเมนของเว็บไซต์ดังกล่าวไปจนกว่าหน่วยงานจะสามารถหาสาเหตุและแก้ไขได้ เพื่อป้องกันการนำไปใช้อันจะส่งผลให้เกิดความเสียหายและเสื่อมเสียชื่อเสียงต่อกระทรวงสาธารณสุข

๓) ช่วยเฝ้าระวังภัยคุกคามทางไซเบอร์ของหน่วยงานในสังกัดกระทรวงสาธารณสุข

๔) ให้หน่วยภายภายใต้กระทรวงสาธารณสุขใช้โดเมนของกระทรวงสาธารณสุข (moph.go,th) ภายใต้การจัดสรรโดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

๕) เป็นหน่วยงานกลางในการสร้าง Community การรักษาความมั่นคงปลอดภัยไซเบอร์ โดยรวมทีม CIRT (Cyber Incident Response Team) ของหน่วยงานในสังกัดกระทรวงสาธารณสุข

๖) กำหนดช่องทางติดต่อ Health CERT

- โทรศัพท์ ๐๘ ๓๐๖๔ ๙๘๖๗
- อีเมล: health-cirt@moph.go.th
- Line Official: @health-cirt
- Line Group: mophCIRT
- เว็บไซต์แจ้งเหตุการณ์ไซเบอร์: https://health-cirt.moph.go.th
- เว็บไซต์เผยแพร่ประชาสัมพันธ์ข้อมูลข่าวสารทางไซเบอร์: https://cyber.moph.go.th/

๓. มาตรการเชิงพื้นที่

หน่วยงานในสังกัดกระทรวงสาธารณสุขดำเนินการ ดังนี้

๑) **สำรวจ**เว็บไซต์ของหน่วยงานตนเองทั้งหมด และจัดทำทะเบียนเว็บไซต์พร้อมด้วย IP Address จัดส่งให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ในฐานะ Health CERT เพื่อนำไปจัดทำทะเบียนเว็บไซต์ของกระทรวงสาธารณสุข

๒) **ปิด**เว็บไซต์ที่ไม่ได้ใช้งานและเว็บไซต์ที่มีความเสี่ยงทั้งหมด เพื่อลดความเสี่ยงในการถูกคุกคามทางไซเบอร์จากผู้ไม่หวังดี

๓) **ดูแล** Environments ทั้งหมดที่เกี่ยวข้อง ของเว็บไซต์ และอัปเดตให้ทันสมัย เช่น อัปเดตเวอร์ชันและ Patch ของ ระบบปฏิบัติการและซอฟต์แวร์ให้เป็นปัจจุบัน เป็นต้น

๔) จัดหาอุปกรณ์**ป้องกัน** เช่น จัดหา Firewall, Web Application Firewall และ Antivirus เป็นต้น

๕) **เฝ้า**ระวังภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง