



ที่ ปน ๐๐๒๓.๑/ว ๖๕๒

ถึง องค์การบริหารส่วนจังหวัดปัตตานี เทศบาลเมืองปัตตานี เทศบาลเมืองตะลุบัน และสำนักงานส่งเสริม
การปกครองท้องถิ่นอำเภอทุกอำเภอ

ด้วย สำนักงานส่งเสริมการปกครองท้องถิ่นจังหวัดปัตตานีได้รับแจ้งจากกรมส่งเสริม
การปกครองท้องถิ่น ว่ามีการแพร่กระจายจากมัลแวร์ประเภทเรียกค่าไถ่ (Ransomware) WannaCry
ซึ่งมีจุดประสงค์เพื่อเข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมดนำมาเรียกค่าไถ่ และหากไม่จ่ายเงิน
จะไม่สามารถเปิดไฟล์ได้ ซึ่งมัลแวร์ประเภทนี้จะกระทำการโจมตีผ่านช่องโหว่ของระบบปฏิบัติการ (Windows)
ที่เกี่ยวข้องกับบริการแชร์ไฟล์ผ่านเครือข่าย (Server Message Block : SMB) ดังนั้น เพื่อเป็นการป้องกัน
และเฝ้าระวังมัลแวร์ดังกล่าว จึงขอให้แจ้งประชาสัมพันธ์ให้บุคลากรในสังกัดและองค์กรปกครองส่วนท้องถิ่น
ได้ทราบแนวทาง ในการป้องกันมัลแวร์ประเภทเรียกค่าไถ่ (Ransomware) WannaCry รายละเอียดปรากฏ
ตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อพิจารณาดำเนินการต่อไป สำหรับสำนักงานส่งเสริมการปกครองท้องถิ่นอำเภอ
ให้แจ้งองค์กรปกครองส่วนท้องถิ่นในเขตพื้นที่ทราบด้วย



สำนักงานส่งเสริมการปกครองท้องถิ่นจังหวัด
ฝ่ายบริหารทั่วไป

โทร. ๐-๗๓๓๔-๔๕๑๙ ต่อ ๑๑๕

โทรสาร ๐-๗๓๓๓-๖๕๘๑



ด่วนที่สุด

บันทึกข้อความ

เลขที่	4175
วันที่	30 พ.ค. 2560
ที่	13 49 น.

ส่วนราชการ ศส. (กลุ่มงานระบบงานคอมพิวเตอร์) โทร. ๐-๒๒๔๑-๙๐๐๐ ต่อ ๑๑๐๕, ๑๑๑๖

ที่ มท ๐๘๐๖.๓/ว ๑๐๑๑

วันที่ ๒๒ พฤษภาคม ๒๕๖๐

เรื่อง การป้องกันและเฝ้าระวังภัยมัลแวร์เรียกค่าไถ่ WannaCry แพร่กระจายผ่านช่องโหว่ของวินโดวส์

เรียน ท้องถิ่นจังหวัดทุกจังหวัด

ด้วยขณะนี้ มีการแพร่กระจายมัลแวร์ประเภทเรียกค่าไถ่ (Ransomware) WannaCry ซึ่งมีจุดประสงค์เพื่อเข้ารหัสลับข้อมูลไฟล์เอกสารและไฟล์สำคัญทั้งหมดนำมาเรียกค่าไถ่ และหากไม่จ่ายเงิน จะไม่สามารถเปิดไฟล์ได้ ซึ่งมัลแวร์ประเภทนี้จะทำการโจมตีผ่านช่องโหว่ของระบบปฏิบัติการ (Windows) ที่เกี่ยวข้องกับบริการแชร์ไฟล์ผ่านเครือข่าย (Server Message Block : SMB) ดังนั้น เพื่อเป็นการป้องกัน และเฝ้าระวังภัยมัลแวร์ดังกล่าว จึงขอให้แจ้งบุคลากรในสังกัดและองค์กรปกครองส่วนท้องถิ่นทราบแนวทางการป้องกันมัลแวร์ประเภทเรียกค่าไถ่ (Ransomware) WannaCry ดังนี้

๑) ระมัดระวังในการคลิก Link และเปิดไฟล์แนบที่มาจากอีเมลทั้งที่ส่งมาทางอีเมล ของ สด. และ free อีเมล เพื่อความปลอดภัย หากจำเป็นต้องเปิดควรตรวจสอบกับผู้ส่งอีเมลว่าได้ส่งอีเมลฉบับนั้นมาจริง

๒) ปรับปรุง (Update) ระบบปฏิบัติการ Microsoft Windows ให้เป็นปัจจุบัน เพื่อป้องกันการ ใช้ช่องโหว่ของระบบเป็นช่องทางให้คอมพิวเตอร์ติดมัลแวร์

๓) ควรสำรองข้อมูลสำคัญออกจากเครื่องคอมพิวเตอร์อย่างสม่ำเสมอ เพื่อความปลอดภัย และป้องกันข้อมูลสูญหายหรือการถูกเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่

จึงเรียนมาเพื่อทราบและพิจารณาดำเนินการต่อไป

(นายคุณุ สุวัฒน์วิทยากร)

รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมส่งเสริมการปกครองท้องถิ่น