ประกาศสำนักบริการวิชาการ มหาวิทยาลัยมหาสารคาม
เรื่อง แนวปฏิบัติขั้นพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware)
และการรั่วไหลของข้อมูล

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

ตามที่ สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้แจ้งให้หน่วยงานรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามแนวปฏิบัติขั้นพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูล สำหรับหน่วยงาน ดังนั้นเพื่อให้เกิดความมั่นคงปลอดภัยมากยิ่งขึ้น สามารถป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามไซเบอร์ได้ สำนักบริการวิชาการจึงประกาศแนวปฏิบัติขั้นพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูล ดังนี้

ข้อ ๑. การสำรองข้อมูลที่สำคัญต่อการดำเนินงาน

๑.๑ ให้สำรองข้อมูลไว้บนคอมพิวเตอร์ที่ทำงาน

๑.๒ ให้สำรองข้อมูลไว้บน Flash drive หรือ Hard disk Drive

๑.๓ ให้สำรองข้อมูลไว้บนระบบ Cloud เช่น Google drive, OneDrive เป็นต้น

๑.๔ ให้สำรองข้อมูลอย่างน้อยเดือนละ ๑ ครั้ง

ข้อ ๒. การกำหนดบัญชีผู้ใช้งาน และการตั้งรหัสผ่านที่สำคัญต่อการดำเนินงาน

๒.๑ ควรตั้งรหัสผ่านอย่างน้อย ๘ ตัว โดยประกอบด้วยตัวอักษรเล็ก(abcd) ตัวอักษรใหญ่(ABCD) ตัวเลข(๑๒๓๔) และสัญลักษณ์ ($#!?) เพื่อสร้างความหลากหลายให้กับรหัสผ่าน

๒.๒ ควรมีการเก็บหรือจัดการกับรหัสผ่านที่มีความปลอดภัยจากการถูกแฮก

๒.๓ ควรหลีกเลี่ยงการตั้งรหัสผ่านเดียวกันหลาย ๆ ระบบ

๒.๔ ควรเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ

๒.๕ ปิดการใช้งาน “hint” หรือคำใบ้รหัสผ่าน

ข้อ ๓. การเปิดใช้งานการยืนยันตัวตนสองครั้ง (Multi-Factor Authentication) สำหรับทุกการใช้งานโดยเฉพาะระบบอีเมลล์ ระบบเครือข่ายภายใน และบัญชีการเข้าใช้งานระบบต่าง ๆ ที่สำคัญ

๓.๑ ผู้ดูแลระบบ(นายธนกฤต ลาวัลย์) เปิดใช้งานการยืนยันตัวตนสองครั้ง ในการเข้าระบบเครื่องมือพัฒนาเว็บไซต์สำนักบริการวิชาการ และเข้าระบบอีเมลล์

๓.๒ บุคลากรเปิดใช้งานการยืนยันตัวตนสองครั้ง ในการเข้าระบบอีเมลล์

/ให้ตรวจสอบ...

ข้อ ๔. ให้ตรวจสอบการอัปเดตแพทต์ของระบบปฏิบัติการและซอฟต์แวร์ รวมถึงติดตั้งโปรแกรมป้องกันมัลแวร์กับคอมพิวเตอร์ทุกเครื่อง โดยผู้ดูแลระบบ(นายธนกฤต ลาวัลย์) จัดทำแผนการตรวจสุขภาพคอมพิวเตอร์ของหน่วยงาน และติดตามการอัตเดตแพทต์ของระบบปฏิบัติการและซอฟต์แวร์ รวมถึงติดตั้งโปรแกรมป้องกันมัลแวร์กับคอมพิวเตอร์ของหน่วยงานทุก ๔ เดือน และรายงานให้ผู้บริหารทราบ

ข้อ ๕. การจัดการสิทธิ์เข้าถึงข้อมูลและทรัพยากรในระบบของหน่วยงาน ตามหลัก Last Privilage โดยนายธนกฤต ลาวัลย์ นักวิชาการคอมพิวเตอร์ เป็นผู้กำหนดสิทธิ์ในการใช้งานและเข้าถึงข้อมูลสำคัญ เช่น บุคลากรสามารถเข้าถึงการแชร์ไดร์ฟข้อมูลการประชุมคณะกรรมการดำเนินงานสำนักบริการวิชาการ

ข้อ ๖. ผู้ดูแลระบบ(นายธนกฤต ลาวัลย์) ต้องเฝ้าระวังและตรวจจับความผิดปกติที่เกิดขึ้นบนระบบเครือข่ายและเครื่องปลายทางอย่างสม่ำเสมอเมื่อเจอความผิดปกติ จะต้องดำเนินการแจ้งความผิดปกติไปยังสำนักคอมพิวเตอร์ทันที

จึงประกาศมาเพื่อทราบโดยทั่วกัน และถือปฏิบัติตามนโยบายอย่างเคร่งครัดต่อไป

ประกาศ ณ วันที่ ๒๑ มีนาคม พ.ศ. ๒๕๖๗

(ผู้ช่วยศาสตราจารย์ธีรยุทธ ชาติชนะยืนยง)
ผู้รักษาการในตำแหน่งผู้อำนวยการสำนักบริการวิชาการ