ภัยไซเบอร์...ภัยใกล้ตัว

ในยุคดิจิทัลที่หน่วยงานราชการนำเทคโนโลยีสารสนเทศมาใช้ในการทำงานมากขึ้น ไม่ว่าจะเป็นระบบสารบรรณอิเล็กทรอนิกส์ อีเมลราชการ หรือฐานข้อมูลต่าง ๆ การทำงานจึงรวดเร็วและมีประสิทธิภาพมากขึ้น แต่ในขณะเดียวกัน “ภัยไซเบอร์” ก็กลายเป็นความเสี่ยงใกล้ตัวที่บุคลากรทุกคนต้องตระหนัก ซึ่งภัยคุกคามทางไซเบอร์คือการเข้าถึงระบบหรือข้อมูลโดยไม่ได้รับอนุญาต เพื่อขโมย ทำลาย หรือรบกวนการทำงานขององค์กร ส่วนการรักษาความมั่นคงปลอดภัยไซเบอร์คือการใช้มาตรการและแนวปฏิบัติเพื่อปกป้องข้อมูลให้มีความลับ ความถูกต้อง และสามารถใช้งานได้อย่างต่อเนื่อง ซึ่งถือเป็นพื้นฐานสำคัญของการทำงานในยุคปัจจุบันภัยไซเบอร์มีหลายรูปแบบ เช่น มัลแวร์ที่แฝงมากับไฟล์หรือเว็บไซต์ แรนซัมแวร์ที่ล็อกไฟล์แล้วเรียกค่าไถ่ ฟิชชิงที่หลอกให้เปิดเผยข้อมูลสำคัญ การโจมตีระบบให้ล่ม รวมถึงความผิดพลาดจากบุคคลภายในองค์กรเอง ไม่ว่าจะตั้งใจหรือไม่ก็ตาม ผลกระทบอาจเกิดได้ทั้งในระดับบุคคล เช่น ข้อมูลส่วนตัวรั่วไหล ถูกหลอกโอนเงิน หรือถูกนำบัญชีไปใช้โดยไม่รู้ตัว และในระดับหน่วยงาน เช่น ระบบหยุดชะงัก ไม่สามารถให้บริการประชาชนได้ สูญเสียความน่าเชื่อถือ และอาจมีความเสียหายทางกฎหมายและการเงินตามมา

อย่างไรก็ตาม ภัยไซเบอร์สามารถลดความเสี่ยงได้ หากทุกคนร่วมกันป้องกันอย่างถูกวิธี เช่น การตั้งรหัสผ่านที่คาดเดายากและไม่ใช้ซ้ำ หลีกเลี่ยงการกดลิงก์หรือเปิดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ ตรวจสอบอีเมลก่อนให้ข้อมูลสำคัญ อัปเดตระบบและโปรแกรมอยู่เสมอ สำรองข้อมูลเป็นประจำ และรีบแจ้งเจ้าหน้าที่ IT เมื่อพบความผิดปกติ เพียงปฏิบัติตามแนวทางพื้นฐานเหล่านี้อย่างสม่ำเสมอ ก็จะช่วยลดโอกาสเกิดความเสียหายได้อย่างมาก และทำให้องค์กรสามารถดำเนินงานได้อย่างมั่นคง ปลอดภัย และมีประสิทธิภาพในระยะยาว

ที่มา (Reference):

- Sangfor. “What is Cyber Threat”
- สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA). “Cybersecurity 101”