นโยบายเพื่อความปลอดภัยข้อมูลและไวรัสคอมพิวเตอร์

ข้อควรปฏิบัติเพื่อความปลอดภัยข้อมูลและไวรัสคอมพิวเตอร์

1. หมั่นอัปเดตวินโดว์หรือระบบปฏิบัติการที่เราใช้รวมไปถึงเว็บเบราว์เซอร์

2. หมั่นทำการ BACKUP สำรองข้อมูล สำรองไฟล์ที่สำคัญบ่อยๆ ซึ่งอาจจะบันทึกลง FLASH DRIVE หรือ EXTERNAL HD

3. หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสมไม่คลิกไฟล์แบบที่ไม่มั่นใจ

4. เช็คที่มาที่ไปของไฟล์ที่จะดาวน์โหลดมาจากอินเทอร์เน็ต และควรทำการสแกนไวรัสทุกครั้ง

5. ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรมแชทต่างๆ หรือช่องทาง SOCIAL MEDIA เพื่อหลีกเลี่ยงการติดมัลแวร์ ซึ่งมัลแวร์มาจากพวกไฟล์แนบทาง SOCIAL NETWORK เพิ่มมากขึ้น

6. ตรวจสอบ E-MAIL ทุกฉบับที่ส่งเข้ามาว่ามาจากบุคคลที่รู้จักหรือไม่ ข้อมูลต้นทาง และปลายทางของ E-MAIL ถูกต้องมีหัวข้อเรื่องที่ติดต่อชัดเจน

7. ควรรอบคอบอย่าประมาทในการทำธุรกรรมใดๆ ผ่านอินเทอร์เน็ต

8. หมั่นตรวจสอบการทำธุรกรรมทางอินเทอร์เน็ต เช่น การจับจ่ายซื้อของผ่านทางอินเทอร์เน็ต หรือการจ่ายค่าสาธารณูปโภคต่างๆ รวมไปถึงดูรายงาน STATEMENT การเข้า – ออก ของเงินหรือเครดิตเพราะถ้าหากเกิดปัญหาใดๆ จะได้แก้ไขได้ทันท่วงที

9. การใช้บริการอินเทอร์เน็ต อย่าตั้งรหัสผ่านเหมือนกันทุกระบบ เพราะหากคุณโดนแฮ็กเกอร์เจาะระบบสำเร็จแล้ว ระบบอื่นๆ ก็อาจถูกเจาะระบบด้วยหากใช้รหัสผ่านเดียวกัน

10. ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และอ่านพิจารณาข้อมูลก่อนการแชร์ต่อ ตลอดจน ไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

สำนักเทคโนโลยีสารสนเทศ

Call : 02 432 6101 ต่อ 1422-1423 http://it.rpu.ac.th