ประกาศโรงเรียนเตรียมอุดมศึกษา
งานศูนย์เทคโนโลยีและการสื่อสาร (ICT)

ตามที่งานศูนย์เทคโนโลยีและการสื่อสาร (ICT) โรงเรียนเตรียมอุดมศึกษา ได้ตรวจพบ SpamMail (สแปมเมล คือ เมลที่ไม่พึงประสงค์) ในระบบ mail server นั้น งานศูนย์เทคโนโลยีและการสื่อสาร (ICT) โรงเรียนเตรียมอุดมศึกษา **จึงขอแจ้งเตือนให้นักเรียนดำเนินการเปลี่ยนพาสเวิร์ดเป็นพาสเวิร์ด "ที่เป็นส่วนตัว" ไม่ควรใช้พาสเวิร์ดที่โรงเรียนตั้งให้เริ่มต้น** เพราะอาจถูกผู้ไม่หวังดีนำอีเมลไปใช้ในทางที่ผิด โดยส่ง SpamMail หรือไวรัสคอมพิวเตอร์ดังกล่าวไปยังอีเมลอื่นมากจนผิดปกติ และถ้าระบบ mail server ตรวจพบ จะดำเนินการล็อค account email ของนักเรียน จึงทำให้นักเรียนไม่สามารถใช้งาน account email ได้

ติดต่อสอบถามได้ที่ Email : ict@triamudom.ac.th

ครูหรือนักเรียนท่านใดที่พบปัญหาดังกล่าวให้ดำเนินการ ดังนี้

1. สแกนไวรัสในเครื่องคอมพิวเตอร์ของตนเองด้วยโปรแกรมแอนตี้ไวรัสก่อน เพื่อให้แน่นใจว่าหลังจากดำเนินการของรีเซต พาสเวิร์ดแล้วจะไม่ติดไวรัสอีกครั้ง
2. ขอรีเซตพาสเวิร์ด Account Email ดังกล่าวผ่านทางหน้าเว็บไซต์โรงเรียน www.triamudom.ac.th หรือที่ลิงค์ https://forms.gle/UtQKdoWQuYai1goR7

ข้อแนะนำ 6 วิธีป้องกันการติดไวรัส มัลแวร์ โทรจัน (Malware Trojans)

หากเปิดพบใน Inbox (อินบล็อค) ของเราได้รับอีเมลแปลก ๆ ที่ไม่รู้ที่มา อ่านชื่อผู้ส่งไม่ออกหรือไม่ใช่ของบุคคลที่เรารู้จัก หรือชื่อเรื่อง อ่านไม่ออก ให้สันนิษฐานว่าเป็น SpamMail (สแปมเมล คือ เมลที่ไม่พึงประสงค์) ให้ลบได้เลย **และที่สำคัญที่สุด คือ พาสเวิร์ดของอีเมลไม่ควรง่ายจนเกินไป**

1. **เปลี่ยนพาสเวิร์ดเป็นพาสเวิร์ด "ที่เป็นส่วนตัว" ไม่ควรใช่พาสเวิร์ดที่โรงเรียนตั้งให้**
2. **อย่าให้หรือโพสต์ที่อยู่อีเมลของคุณสู่สาธารณะ**

ควรจำไว้ว่าทุกคนสามารถเข้าถึงอินเทอร์เน็ตได้อย่างง่ายดาย นั่นหมายความว่าผู้ส่งอีเมลขยะยังแฝงตัวอยู่ในอินเทอร์เน็ต และค้นหาที่อยู่อีเมล์ ตามแหล่งต่างๆ ด้วยเครื่องมือดูดอีเมล์ตามเว็บไซต์ มาเพื่อการส่งสแปมเมล์ แย่ไปกว่านั้นเขาอาจสามารถทำการแฮ็คบัญชีของคุณหากคุณใช้รหัสผ่านที่อ่อนแอ

3. **คิดก่อนคลิก**

ตรวจสอบให้แน่ใจก่อนเปิดไฟล์แนบใด ๆ แม้ว่าจะดูเหมือนไฟล์ข้อความหรือรูปภาพที่น่าสนใจขนาดไหน หรือคลิกที่ไฮเปอร์ลิงก์ หลีกเลี่ยงการดาวน์โหลดเนื้อหาที่ถูกบล็อก ส่วนใหญ่อีเมลเหล่านี้มักจะอยู่ในกล่อง "สแปม" อยู่แล้ว

4. **อย่าตอบกลับข้อความสแปม**

ข้อความสแปมเกือบทั้งหมดเป็นอีเมลที่เป็นอันตรายที่ส่งมาจากแหล่งที่ไม่รู้จัก แหล่งข้อมูลเหล่านี้อาจเป็นแฮกเกอร์ที่ต้องการเจาะเข้าสู่คอมพิวเตอร์ของคุณ อย่าตอบกลับข้อความสแปมเพราะผู้ส่งสแปมจะรู้ว่าที่อยู่อีเมลนั้นมีการใช้งานและจะเพิ่มโอกาสของอีเมลของคุณที่จะถูกกำหนดเป้าหมายอย่างต่อเนื่องโดยผู้ส่งสแปม

5. **ใช้เครื่องมือกรองสแปม หรือ ซอฟต์แวร์ป้องกันไวรัส**

เครื่องมือกรองสแปม หรือ ซอฟต์แวร์ป้องกันไวรัสสามารถช่วยสแกนอีเมลที่คุณได้รับจากมัลแวร์ หากอีเมลที่คุณได้รับมีมัลแวร์เนื้อหาที่เป็นอันตรายจะถูกกักกันและคุณจะถูกป้องกันไม่ให้เปิด วิธีนี้จะช่วยลดโอกาสที่อีเมลที่มีมัลแวร์ติดไวรัสในคอมพิวเตอร์ของคุณ เครื่องมือกรองสแปม หรือ ซอฟต์แวร์ป้องกันไวรัส จะมีคุณสมบัติในการถอดรหัสเนื้อหาอีเมลและปิดกั้นสแปมก่อนถึงมือคุณ

6. **ห้ามใช้เมลส่วนตัว หรือ เมลองค์กรของคุณลงทะเบียนออนไลน์ กับเว็บไซต์ที่ไม่น่าเชื่อถือ**

ก่อนลงทะเบียน ออนไลน์ หรือทำธุรกรรมต่างๆ ออนไลน์ ควรตรวจสอบให้มั่นใจก่อน ว่ามีความปลอด ถ้าต้องการสมัครกิจกรรมที่ไม่ค่อยสำคัญควร **มีอีเมลสำรอง**