10 คำแนะนำป้องกันทาง **E-mail**		
1. ตั้งค่า password ที่คาดเดาได้ยาก และมั่นเปลี่ยนบ่อยๆ	2. ดูแลช่องทางที่ใช้ในการ Reset รหัสผ่านให้มีความมั่นคงปลอดภัย เช่น อีเมลสำรองสำหรับกู้คืนบัญชี	3. ตรวจสอบประวัติการใช้งานที่น่าสงสัยรวมถึงช่องทางในการยืนยันตัวตนอย่างสม่ำเสมอ
4. ติดตั้งโปรแกรมป้องกันไวรัส และหมั่นอัพเดตระบบปฏิบัติการ เบราว์เซอร์ และซอฟต์แวร์ให้ทันสมัย	5. หลีกเลี่ยงการใช้เว็บเมลผ่านเครื่องคอมพิวเตอร์สาธารณะและไม่ควรตั้งค่าให้เครื่องจำรหัสผ่าน	6. ระมัดระวังอีเมลที่มีไฟล์แนบหรือลิงก์พาไปเว็บอื่น
7. แม้อีเมลจากคนที่รู้จักก็อาจจะเป็นคนร้ายปลอมตัวมาก็ได้ หากไม่แน่ใจควรยืนยันผ่านช่องทางอื่นที่ไม่ใช่อีเมล เช่น แจ้งยืนยันเปลี่ยนเลขที่บัญชีโอนเงินทางโทรศัพท์	8. เปิดการใช้งานยืนยันตัวตนแบบ 2 Factor Authentication โดยใช้เบอร์โทรศัพท์ อีเมลสำรอง หรือโปรแกรม เช่น Google Authentication	9. เช็ครายชื่อผู้ที่จะได้รับอีเมลก่อนกดปุ่ม Reply หรือ Reply All ทุกครั้ง เพราะผู้ร้ายมักจะใช้เทคนิคตั้งชื่ออีเมลให้ใกล้เคียงกับคนที่เรารู้จัก
10. อย่าหลงเชื่ออีเมลที่หลอกให้เปลี่ยนรหัสผ่าหรือให้อัพเดตข้อมูลส่วนตัว หากไม่แน่ใจควรสอบถามกับผู้ที่ส่งข้อมูลมาในช่องทางอื่นๆ อีกครั้ง	*ข้อมูลจาก : ThaiCert* *จัดทำโดย : กลุ่มระบบคอมพิวเตอร์และเครือข่ายความมั่นคง กองสารสนเทศนิติวิทยาศาสตร์*	