

สรุปการแลกเปลี่ยนเรียนรู้

หัวข้อ : “เตือนภัยไซเบอร์ สังเกตและคิดก่อนคลิกลิงค์ เพื่อความปลอดภัย”

วัน/เดือน/ปี 14 กรกฎาคม 2566 สถานที่ กลุ่มพัฒนาระบบบริหาร กรมอนามัย เวลา ...10.00 - 10.30 น.

ผู้สรุป.....นางสาวจุฬาลักษณ์ เก่งการช่าง.....ตำแหน่ง.....นักวิเคราะห์นโยบายและแผนปฏิบัติการ.....

เผยแพร่ข้อมูลโดย : กลุ่มพัฒนาระบบบริหาร กรมอนามัย

❖ สรุปการแลกเปลี่ยนเรียนรู้ 🚨 เตือนภัยไซเบอร์ ป้องกันข้อมูลส่วนบุคคลรั่วไหล !!!

➢ วิธีป้องกันข้อมูลส่วนบุคคลรั่วไหล เพื่อให้เกิดความปลอดภัยของข้อมูลส่วนบุคคล

- 1 หากพบว่ามีการก่อความทู่ทางโทรศัพท์ SMS หรือ Line ให้ Block แล้วแจ้งผู้ให้บริการ
- 2 มือถือและอุปกรณ์คอมพิวเตอร์ ควร update และติดตั้งโปรแกรมป้องกันไวรัส
- 3 ตรวจสอบการล็อกอินบัญชี หรือประวัติการเชื่อมต่อเข้ามาใช้งานบัญชีต่าง ๆ
- 4 ติดตามธุรกรรมทางการเงิน และเปิดระบบแจ้งเตือนของธนาคาร เมื่อมีรายการผิดปกติเกิดขึ้นให้รีบติดต่อธนาคารทันที
- 5 เปลี่ยนรหัสผ่านใหม่ที่ใช้ในการเข้าระบบ หากใช้รหัสชุดเดียวกันทุกระบบ ต้องเปลี่ยนไม่ควรใช้ซ้ำกัน
- 6 ระมัดระวังการให้ข้อมูลส่วนบุคคล หรือ แก๊งคอลเซ็นเตอร์ แอบอ้างนำข้อมูลไปใช้ทำให้เกิดความเสียหาย
- 7 ใช้การยืนยันตัวตนสองชั้นตอน (Two-factor Authentication) ในการ Login เข้าใช้งานระบบต่าง ๆ
- 8 แชรความรู้ต่อให้ผู้อื่นรู้เท่าทันกลลวงไม่ให้ตกเป็นเหยื่อของมิจฉาชีพอีกต่อไป
- 9 หากพบเจอความผิดปกติหรือน่าสงสัย ให้ติดต่อสอบถามข้อมูลกับหน่วยงานที่เกี่ยวข้องโดยตรง



ข้อมูลส่วนบุคคล รั่วไหล ทำอย่างไร ?

- 1 หากพบว่ามีการก่อความทู่ทางโทรศัพท์ SMS หรือ Line ให้ Block แล้วแจ้งผู้ให้บริการ
- 2 มือถือและอุปกรณ์คอมพิวเตอร์ ควร update และติดตั้งโปรแกรมป้องกันไวรัส
- 3 ตรวจสอบการล็อกอินบัญชี หรือประวัติการเชื่อมต่อเข้ามาใช้งานบัญชีต่าง ๆ
- 4 ติดตามธุรกรรมทางการเงิน และเปิดระบบแจ้งเตือนของธนาคาร เมื่อมีรายการผิดปกติเกิดขึ้นให้รีบติดต่อธนาคารทันที
- 5 เปลี่ยนรหัสผ่านใหม่ที่ใช้ในการเข้าระบบ หากใช้รหัสชุดเดียวกันทุกระบบ ต้องเปลี่ยนไม่ควรใช้ซ้ำกัน
- 6 ระมัดระวังการให้ข้อมูลส่วนบุคคล หรือ แก๊งคอลเซ็นเตอร์ แอบอ้างนำข้อมูลไปใช้ทำให้เกิดความเสียหาย
- 7 ใช้การยืนยันตัวตนสองชั้นตอน (Two-factor Authentication) ในการ Login เข้าใช้งานระบบต่าง ๆ
- 8 แชรความรู้ต่อให้ผู้อื่นรู้เท่าทันกลลวงไม่ให้ตกเป็นเหยื่อของมิจฉาชีพอีกต่อไป
- 9 หากพบเจอความผิดปกติหรือน่าสงสัย ให้ติดต่อสอบถามข้อมูลกับหน่วยงานที่เกี่ยวข้องโดยตรง

find สามารถแจ้งเหตุฉุกเฉินทางไซเบอร์ได้ที่ thaicert@ncsa.or.th

โปรดระวัง มิจฉาชีพ ส่ง SMS หรือไลน์ มาให้กดลิงก์แนบ หากเหยื่อหลงเชื่อกดลิงก์ !! อาจถูกขโมยข้อมูลสำคัญหรือเงินในบัญชีได้



เตือน!!! อย่า Click Link ใน SMS
แม้จะมาใน Inbox ของธนาคาร

หากพบ SMS ปลอมตัวให้สงสัย ให้รีบแจ้งผู้ให้บริการ SMS ของธนาคารภายใน 24 ชม. ไม่ควรแชร์หรือส่งต่อข้อความดังกล่าวให้ผู้อื่นได้ หรือใช้ข้อมูลใน SMS นั้นๆ

กรมการสื่อสารโทรคมนาคม
ออกบริการ SMS แบบเบ็ดเสร็จแล้ว ถ้าเจออย่าแชร์อย่าให้คนอื่น!

อย่าเชื่อ อย่ารับ อย่าโอน

มีงานวิจัยพบว่า 90% ของการโจมตีทางไซเบอร์ เกิดขึ้นจาก SMS ปลอมตัว

เว็บไซต์กรมสอบสวนคดีพิเศษ
www.dsigo.th

เว็บไซต์กรมสอบสวนคดีพิเศษ
www.dsigo.th



ขอให้สังเกตและคิด ก่อนคลิก ทุกครั้ง เพื่อความปลอดภัย

ไม่เชื่อ ไม่รับ ไม่โอน



แจ้งเหตุภัยคุกคามทางไซเบอร์ ได้ที่ thaicert@ncsa.or.th

โทร 02 114 3531

ID : @ncert_ncsa



7 วิธีป้องกัน ปลอดภัยจาก Ransomware

มีสติ รู้เท่าทัน พร้อมป้องกัน Ransomware

แรนซัมแวร์ มาจากไหนได้บ้าง?

- Mail ปลอม ส่งลวงให้โหลดไฟล์แนบ
- Link ปลอม ส่งลวงให้กด ไตร่ตรอง
- Web ปลอม ส่งลวงให้โหลดโปรแกรมฟรี

- 1 สำรอง ข้อมูล Backup File ตามกฎ 3-2-1 Backup Rule อย่างน้อย 3 ชุด โดยใช้ 2 เทคโนโลยีในการสำรองข้อมูลเป็นอย่างน้อย และเก็บ 1 ชุดในที่ปลอดภัยแยกออกจากระบบแบบออฟไลน์
- 2 ไม่คลิก Link จาก Website ปลอมที่ไม่น่าไว้ใจ
- 3 ไม่เปิด File ที่แนบมาจากอีเมลที่ไม่รู้จัก
- 4 อัปเดต ซอฟต์แวร์ให้เป็น Version ปัจจุบัน
- 5 ติดตั้ง โปรแกรมป้องกันมัลแวร์ (Anti-malware) และ อัปเดตอย่างสม่ำเสมอ
- 6 เปิดใช้ Multi-Factor Authentication (MFA) ในการเข้าถึงระบบ RDP, VPN หรืออุปกรณ์ต่าง ๆ
- 7 แยก Account ผู้ใช้งานระหว่าง Admin กับ ผู้ใช้งานทั่วไป

find : www.techhub.or.th

❖ ประโยชน์จากการแลกเปลี่ยนเรียนรู้

1. สร้างความรู้ ความเข้าใจ เกี่ยวกับความปลอดภัยทางไซเบอร์ และการป้องกันข้อมูลส่วนบุคคลรั่วไหล รวมถึงแนวทางรับมือกับภัยคุกคามทางไซเบอร์
2. แลกเปลี่ยนประสบการณ์และความเข้าใจรูปแบบการหลอกลวง กลโกง อาทิ SMS ปลอม เว็บปลอม ภัยแก๊งคอลเซ็นเตอร์ เพื่อรับมือ ป้องกัน และลดความเสี่ยงจากภัยออนไลน์ ไม่ให้ตกเป็นเหยื่อของมิจฉาชีพ