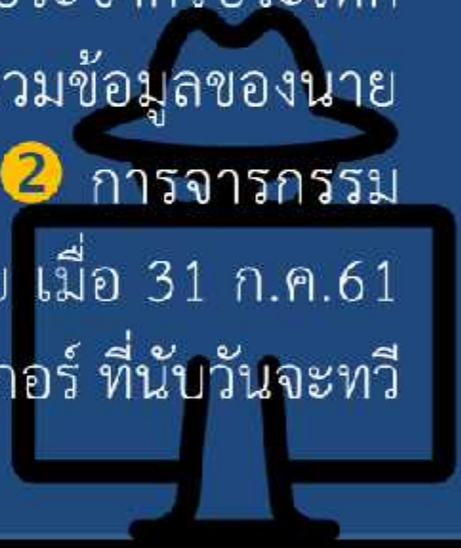
กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ
Directorate of Information and Communication Technology

แจ้งเตือนภัย ความรู้ด้านไซเบอร์ ข้อควรปฏิบัติ/ข้อควรระวัง

การยกระดับการรักษาความปลอดภัยไซเบอร์ ทอ. !!!

สถานการณ์ : จากเหตุการณ์ ❶ การจารกรรมข้อมูลด้านสุขภาพของประชากรประเทศสิงคโปร์ ซึ่งเป็นข้อมูลในระบบคนไข้กลาง SingHealth กว่า 1.5 ล้านราย (รวมข้อมูลของนายลี เซียน ลุง นายกรัฐมนตรีประเทศสิงคโปร์) เมื่อ 20 ก.ค.61 และเหตุการณ์ ❷ การจารกรรมข้อมูลลูกค้าของธนาคารกรุงไทยและธนาคารกสิกรไทย กว่า 1 แสนราย เมื่อ 31 ก.ค.61 นับเป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการเจาะระบบ (Hacking) ของแฮกเกอร์ ที่นับวันจะทวีความรุนแรง และมุ่งเป้าไปที่องค์กรสำคัญในระดับประเทศ



ทำให้ กองทัพอากาศ โดยกำลังพลทุกระดับ ต้องร่วมกันรักษาความปลอดภัยไซเบอร์ทั้งระดับหน่วยงานและระดับบุคคล ด้วยการปฏิบัติตาม “ข้อควรปฏิบัติด้านการรักษาความปลอดภัย” อย่างเคร่งครัด

กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (โทร 2-6394)

แจ้งเตือนภัย ความรู้ด้านไซเบอร์ ข้อควรปฏิบัติ/ข้อควรระวัง

ข้อควรปฏิบัติด้านการรักษาความปลอดภัย

❍ ด้านบุคลากร (Peopleware)

การปฏิบัติทั่วไป

1. ตรวจสอบและเฝ้าระวังการผ่านเข้า-ออกของบุคคลภายนอก ในเขตพื้นที่สารสนเทศของหน่วย
2. เปลี่ยนรหัสผ่าน (Password) ของบัญชีอีเมล ทอ.และของบัญชีใช้งานระบบสารสนเทศใน ทอ.อื่น (ถ้ามี) ตามมาตรฐานความปลอดภัย (ความยาวไม่ต่ำกว่า 8 ตัวอักษร และประกอบไปด้วยอักษรตัวใหญ่, ตัวเล็ก, ตัวเลข และตัวอักษรพิเศษ) พร้อมกำหนดวงรอบการเปลี่ยนรหัสผ่านอย่างน้อย 6 เดือน/ครั้ง
3. ไม่ใช้บัญชีอีเมล ทอ.ในการสมัครเข้าใช้บริการระบบสารสนเทศภายนอก
4. ไม่ตั้งค่ารหัสผ่าน (Password) บัญชีการใช้งานระบบสารสนเทศภายนอก เป็นค่าเดียวกับรหัสผ่านของบัญชีผู้ใช้งานระบบสารสนเทศใน ทอ.
5. ไม่เขียนแสดงรหัสผ่าน (Password) ไว้ในที่ซึ่งสามารถมองหรือสังเกตเห็นได้ และไม่ควรใช้วิธีเขียนจดบันทึกค่ารหัสผ่านโดยตรง ให้ใช้วิธีจดจำหรือเขียนแสดงเป็นคำบอกคำใบ้ (Hint) และจัดเก็บในที่ปลอดภัย

แจ้งเตือนภัย ความรู้ด้านไซเบอร์ ข้อควรปฏิบัติ/ข้อควรระวัง

ข้อควรปฏิบัติด้านการรักษาความปลอดภัย

❍ ด้านบุคลากร (Peopleware)

<u>การปฏิบัติทั่วไป</u>

6. ออกจากหน้าจอการใช้งานคอมพิวเตอร์ (Log Off) ทุกครั้ง ที่ละภารกิจจากเครื่องคอมพิวเตอร์ หรือเปิดใช้งานระบบ Screen Saver แบบต้องป้อนรหัสผ่าน (Password) เมื่อจะเข้าใช้งาน โดยตั้งให้ทำการล็อคหน้าจออัตโนมัติเมื่อไม่มีการใช้งานเป็นระยะเวลา 15 นาทีหรือน้อยกว่า
7. ออกจากระบบการให้บริการทางสารสนเทศ (Log Out) ทุกครั้งที่เสร็จสิ้นการใช้งาน โดยเฉพาะเมื่อใช้งานบนเครื่องคอมพิวเตอร์อื่นที่มิใช่ใช้งานเฉพาะส่วนบุคคล และเมื่อใช้งานบนอุปกรณ์สื่อสารแบบพกพา (ไม่ Login ค้างไว้)
8. ไม่ใช้บริการเชื่อมต่อพรีอินเทอร์เน็ตไร้สายสาธารณะ (Public Free Wi-Fi) ที่มีความเสี่ยง หรือไม่รู้จัก หรือสงสัยว่าอาจเป็นข่ายให้บริการปลอม โดยเฉพาะในต่างประเทศ เพราะอาจถูกดักจับข้อมูลได้

แจ้งเตือนภัย ความรู้ด้านไซเบอร์ ข้อควรปฏิบัติ/ข้อควรระวัง

ข้อควรปฏิบัติด้านการรักษาความปลอดภัย

❍ ด้านบุคลากร (Peopleware)

<u>การปฏิบัติทั่วไป</u>

9. เปิดใช้งานระบบตรวจสอบและยืนยันตัวตนผู้ใช้งาน (User Authentication) ของอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภท Smart Phone และ Tablet เช่น รหัสผ่าน (Password), รหัสวลีผ่าน (Passphrase), โค้ดผ่าน (Passcode), PIN, ลายนิ้วมือ, Face ID และเลือกใช้เป็นการยืนยันตัวตนแบบพหุปัจจัย (Multi-factor Authentication) (ถ้ามี)
10. ไม่เปิดอีเมล/ไม่คลิกลิงค์แนบ/ไม่เปิดไฟล์แนบ ที่มาจากแหล่งที่ไม่รู้จัก
11. ไม่เปิดเว็บไซต์ประเภทลามกอนาจาร เว็บไซต์ที่เสนอโปรแกรมที่ไม่ถูกลิขสิทธิ์ และเว็บไซต์ให้บริการประเภทอื่นที่มิใช่ของผู้ให้บริการอย่างเป็นทางการที่เชื่อถือได้ เพราะมีความเสี่ยงต่อการติดมัลแวร์สูง

แจ้งเตือนภัย ความรู้ด้านไซเบอร์ ข้อควรปฏิบัติ/ข้อควรระวัง

ข้อควรปฏิบัติด้านการรักษาความปลอดภัย

❍ ด้านบุคลากร (Peopleware)

<u>การปฏิบัติทั่วไป</u>

12. สมัครใช้บริการการแจ้งเตือนทาง SMS หรือ อีเมล เมื่อมีการเคลื่อนไหวทางการเงินในบัญชีเงินฝาก
13. ทำลายเอกสารประเภท ใบแจ้ง, บิล, สลิป ที่มีข้อมูลส่วนบุคคลที่สำคัญ (ชื่อ, ที่อยู่, หมายเลขโทรศัพท์, หมายเลขบัตร, หมายเลขประจำตัวประชาชน ฯลฯ) เขียนบรรจุอยู่ ก่อนทิ้งเป็นขยะ
14. เข้ารหัสข้อมูลสำคัญในอุปกรณ์จัดเก็บข้อมูล หรือเข้ารหัสอุปกรณ์จัดเก็บข้อมูล
15. สำรองข้อมูลสำคัญ (Data Backup) และอัพเดทให้เป็นปัจจุบันไว้เสมอ
16. ใช้งานระบบอินเทอร์เน็ตในหน่วยงานเพื่อวัตถุประสงค์ทางราชการเท่านั้น
17. แจ้ง น.รปภ.ระบบสารสนเทศ/น.เทคโนโลยีสารสนเทศ ของหน่วยทันทีที่ตรวจพบสิ่งผิดปกติทางระบบสารสนเทศและการใช้งาน

แจ้งเตือนภัย ความรู้ด้านไซเบอร์ ข้อควรปฏิบัติ/ข้อควรระวัง

ข้อควรปฏิบัติด้านการรักษาความปลอดภัย

❍ ด้านบุคลากร (Peopleware)

<u>การใช้สื่อสังคมออนไลน์</u>

1. ไม่กรอกข้อมูลสำคัญส่วนบุคคล เช่น ยศ, ชื่อ-นามสกุล, ที่อยู่, หมายเลขโทรศัพท์, วันเดือนปีเกิด ฯลฯ ในการเข้าร่วมเล่นเกม, แสดงความคิดเห็น, ใช้บริการ, สั่งซื้อสินค้า, ตอบคำถามร่วมสนุก กับบริการแบบออนไลน์หรือในเครือข่ายสังคมออนไลน์ ซึ่งมีความเสี่ยงต่อการถูกโจรกรรมข้อมูลไปใช้ในทางแสวงประโยชน์อื่น
2. ไม่โพสต์เผยแพร่ข้อมูลสำคัญ เช่น หมายเลขประจำตัวประชาชน, หมายเลขบัตรเครดิต, พาสปอร์ต, ตั๋วเครื่องบิน ฯลฯ ในเครือข่ายสังคมออนไลน์
3. ไม่กดรับคำร้องขอเป็นเพื่อนจากคนที่ไม่รู้จักในเครือข่ายสังคมออนไลน์ และให้ตรวจสอบประวัติกิจกรรมออนไลน์ของผู้ส่งคำร้องขอเป็นเพื่อน ก่อนรับทุกครั้ง
4. ไม่หลงเชื่อการโฆษณาขายสินค้าหรือบริการหลอกลวงแบบออนไลน์ที่เสนอราคาถูกเกินจริง และไม่หลงเชื่อการชักชวนทำธุรกิจ/ธุรกรรมการเงินหลอกลวง แบบเสนอผลตอบแทนสูงเป็นสิ่งล่อใจ

แจ้งเตือนภัย ความรู้ด้านไซเบอร์ ข้อควรปฏิบัติ/ข้อควรระวัง

ข้อควรปฏิบัติด้านการรักษาความปลอดภัย

❍ ด้านบุคลากร (Peopleware)

การใช้สื่อสังคมออนไลน์

5. เปิดใช้งานระบบตรวจสอบตัวตนผู้ใช้งานแบบทวิปัจจัย (Two-factor Authentication) ของบริการแบบออนไลน์ (ถ้ามี)
6. คิดพิจารณาให้รอบคอบก่อนโพสต์ หรือส่งต่อ หรือแสดงความคิดเห็นใด ๆ ในเครือข่ายสังคมออนไลน์

แจ้งเตือนภัย ความรู้ด้านไซเบอร์ ข้อควรปฏิบัติ/ข้อควรระวัง

ข้อควรปฏิบัติด้านการรักษาความปลอดภัย

ด้านเทคโนโลยี (Technology)

1. ทำการอัพเดท Patch ของระบบปฏิบัติการและระบบป้องกันไวรัส/มัลแวร์ให้เป็นปัจจุบันเสมอ
2. เปลี่ยนรหัสผ่าน Wi-Fi ของทุกจุดที่เปิดให้บริการเชื่อมต่อเครือข่ายไร้สาย โดยใช้รูปแบบการเข้ารหัสความปลอดภัยแบบ WPA2 และเป็นไปตามมาตรฐานความปลอดภัย (ความยาวไม่ต่ำกว่า 8 ตัวอักษร และประกอบไปด้วยอักษรตัวใหญ่, ตัวเล็ก, ตัวเลข และตัวอักษรพิเศษ) พร้อมกำหนดวงรอบการเปลี่ยนรหัสผ่านอย่างน้อย 6 เดือน/ครั้ง
3. ไม่ตั้งค่าให้แอพพลิเคชั่นจดจำชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) หรือเข้าสู่ระบบแบบอัตโนมัติ (Automatic Sign-in)
4. ผู้ดูแลระบบตรวจสอบข้อมูลจราจรคอมพิวเตอร์ (Log File) เพื่อเฝ้าระวังการบุกรุกโจมตีและเหตุการณ์ที่ผิดปกติ

แจ้งเตือนภัย ความรู้ด้านไซเบอร์ ข้อควรปฏิบัติ/ข้อควรระวัง

ข้อควรปฏิบัติด้านการรักษาความปลอดภัย

❍ ด้านขั้นตอนและระเบียบปฏิบัติ (Procedure)

1. แจ้งเตือนกำลังพลทุกระดับในหน่วยงานถึงข้อควรปฏิบัตินี้เป็นระยะ
2. จัดทำสื่อเผยแพร่ประชาสัมพันธ์ภายในหน่วยงาน เพื่อกระตุ้นเตือนและยกระดับความตระหนักรู้ด้านความปลอดภัยไซเบอร์ของกำลังพลหน่วย
3. ตรวจสอบและประเมินผลการปฏิบัติ พร้อมทั้งปรับปรุงการกำกับดูแลกำลังพลในหน่วยงานด้านการปฏิบัติอย่างต่อเนื่อง
4. ให้รายงาน ทสส.ทอ.ทราบทันที เมื่อหน่วยได้รับภัยคุกคามทางไซเบอร์