คู่มือ คนไทย รู้ทันภัยไซเบอร์

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

GO DIGITAL with ETDA

GO DIGITAL with ETDA

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งต่อภาครัฐ ภาคธุรกิจเอกชน และภาคประชาชน จึงได้มอบหมายให้ **สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) หรือ ETDA** จัดทำ **คู่มือ "คนไทย รู้ทันภัยไซเบอร์"** ขึ้น เพื่อให้คนไทย ได้ตระหนักถึงปัญหาภัยคุกคามทางออนไลน์รูปแบบต่าง ๆ มีแนวทางในการป้องกันตนเองก่อนตกเป็นเหยื่อ ป้องกันไม่ให้ข้อมูลสำคัญรั่วไหลก่อนผู้ไม่ประสงค์ดีจะนำไปใช้สร้างความเสียหาย และสร้างสรรค์สังคมดิจิทัลที่ทุกคนสามารถใช้ประโยชน์จากเทคโนโลยีได้อย่างมั่นคงปลอดภัยร่วมกัน

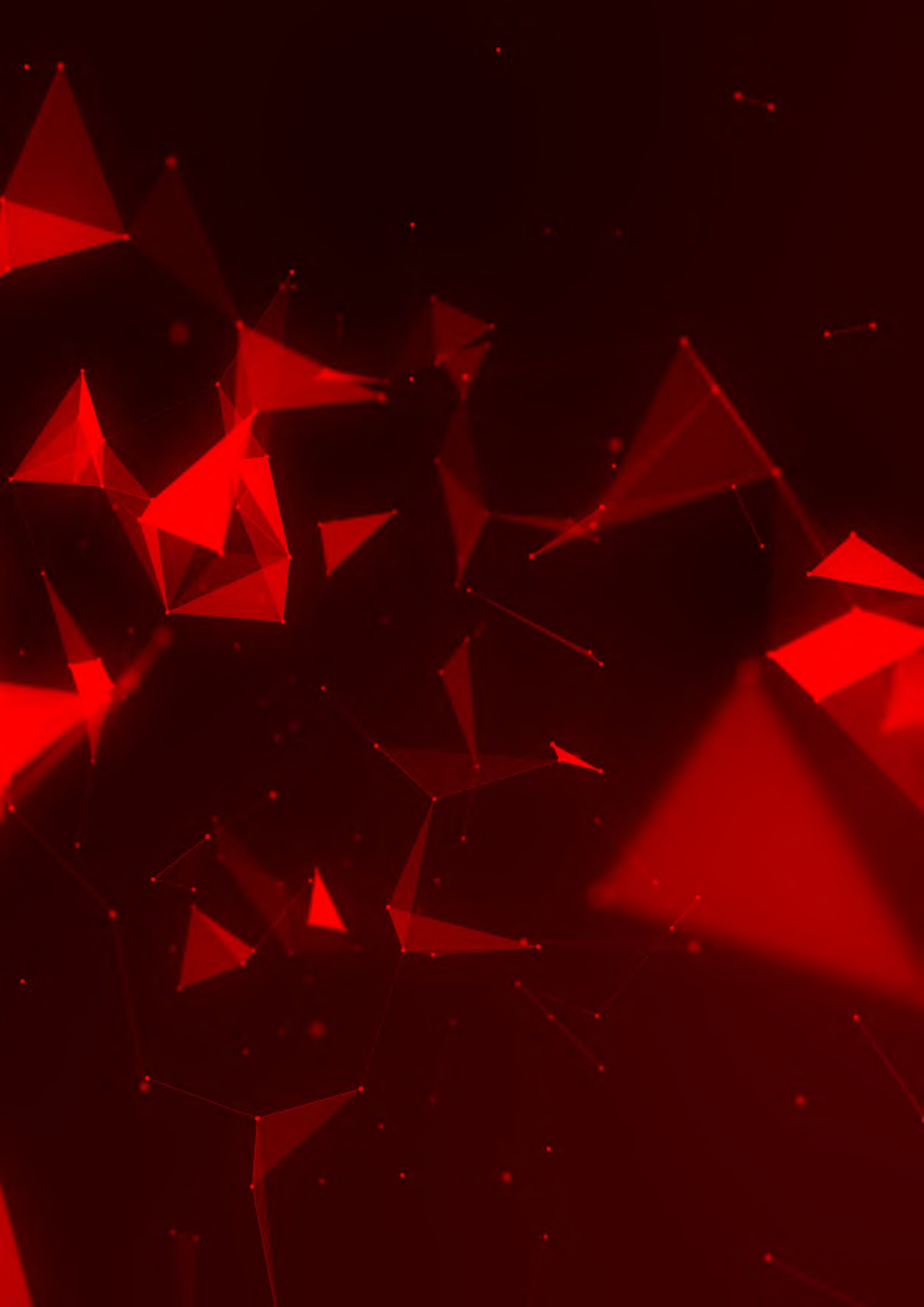
พุทธิพงษ์ ปุณณกันต์
รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

สารบัญ

ติดตามข่าวสารการแจ้งเตือนและข้อแนะนำด้านความมั่นคงปลอดภัยไซเบอร์
เว็บไซต์ : www.thaicert.or.th
เฟซบุ๊ก : www.facebook.com/thaicert

ปรึกษาเพื่อขอคำแนะนำเพิ่มเติมเพื่อเตรียมพร้อมหรือเมื่อเกิดเหตุภัยคุกคาม
โทรศัพท์ : 0-2123-1212
อีเมล
ติดต่อเรื่องทั่วไป office@thaicert.or.th
แจ้งเหตุภัยคุกคาม report@thaicert.or.th

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA



รู้ทัน ป้องกันด้วยพาสเวิร์ด

ต้องทำ

- ใช้แบบไม่ซ้ำในทุกบริการที่ใช้
- มีความยาวอย่างน้อย 8 ตัวอักษร
- ติดตามข่าวสารและเปลี่ยนเมื่อได้รับแจ้งว่าข้อมูลรั่ว

ควรทำ

- ทำให้ซับซ้อนด้วยตัวเลขหรืออักขระพิเศษ

- จดบันทึกและซ่อนไว้ไม่ให้ใครเห็นนั้นทำได้ แต่ทางที่ดี ควรใช้โปรแกรม Password Manager

- เปิดใช้งานการล็อกอินแบบหลายชั้น

ไม่ควรทำ

- ใช้คำที่คาดเดาได้ง่าย เช่น ชื่อ, เบอร์โทร.
- ใช้แป้นตัวอักษรเรียงกัน เช่น qwerty, 123456
- ตั้งเป็นภาษาไทยแต่พิมพ์ด้วยแป้นภาษาอังกฤษ
- บอกให้คนอื่นรู้

GO DIGITAL with ETDA

แนวทางการใช้รหัสผ่าน หรือ พาสเวิร์ด (Password) ให้มั่นคงปลอดภัย กับหลัก "ต้องทำ" "ควรทำ" และ "ไม่ควรทำ"

"ต้องทำ"

- ใช้พาสเวิร์ดแบบไม่ซ้ำในทุกบริการที่ใช้
- ตั้งพาสเวิร์ดให้มีความยาวอย่างน้อย 8 ตัวอักษร
- ติดตามข่าวสารและเปลี่ยนพาสเวิร์ด เมื่อได้รับแจ้งว่าข้อมูลรั่ว

"ควรทำ"

- เพิ่มความซับซ้อนของพาสเวิร์ด เช่น ตัวเลขหรืออักขระพิเศษ
- จดบันทึกและซ่อนพาสเวิร์ดไว้ไม่ให้คนอื่นเห็นนั้นทำได้ แต่ทางที่ดีควรใช้โปรแกรม Password Manager
- เปิดใช้งานการล็อกอินแบบหลายชั้น เช่น การใช้ร่วมกับ OTP หรือการยืนยันตัวตนหลายปัจจัย

"ไม่ควรทำ"

- ตั้งพาสเวิร์ดโดยใช้คำที่คาดเดาได้ง่าย เช่น ชื่อหรือเบอร์โทร.
- ตั้งพาสเวิร์ดโดยใช้แป้นตัวอักษรเรียงกัน เช่น qwerty หรือ 123456
- ตั้งพาสเวิร์ดเป็นภาษาไทยแต่พิมพ์ด้วยแป้นภาษาอังกฤษ
- บอกพาสเวิร์ดให้คนอื่นรู้

นอกจากนี้ Center for Internet Security (CIS) องค์กรที่กำหนดเกณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ ที่ได้รับการยอมรับและนำไปใช้อ้างอิงในหลายหน่วยงาน ได้อัปเดตไกด์ไลน์เรื่องการใช้พาสเวิร์ด เช่น

- ไม่บังคับให้ผู้ใช้ต้องเปลี่ยนพาสเวิร์ดบ่อย ๆ แต่ให้เปลี่ยนเฉพาะในกรณีที่จำเป็น เช่น พบว่าข้อมูลรั่วไหล หรือพบการล็อกอินที่ผิดปกติ อย่างไรก็ตาม ทาง CIS ได้แนะนำให้เปลี่ยนพาสเวิร์ดใหม่ทุก 1 ปี ด้วยเหตุผลว่าเป็นหนทางสุดท้าย (Backstop) ในการรักษาความมั่นคงปลอดภัยของพาสเวิร์ด
- ในขั้นตอนการตั้ง ต้องตรวจสอบว่าไม่ตรงกับรายการที่เคยรั่วไหลมาก่อนหน้านี้ และไม่ซ้ำกับพาสเวิร์ด 5 ชุดล่าสุดที่ผู้ใช้เคยตั้งมาแล้วก่อนหน้านี้
- ตั้งค่าล็อก เมื่อไม่มีการใช้งานเกิน 15 นาทีหรือน้อยกว่า
- ป้องกันการโจมตีแบบเดาพาสเวิร์ด (Brute Force) ด้วยการจำกัดจำนวนครั้งที่ล็อกอินผิด เช่น เมื่อล็อกอินผิดต่อเนื่องเกิน 5 ครั้งให้ระงับการใช้งานบัญชีนั้นชั่วคราว (อย่างน้อย 15 นาที) รวมถึงตั้งค่าให้มีการแจ้งเตือนผู้ดูแลระบบเมื่อมีการล็อกอินผิดพลาดเกินจำนวนครั้งที่กำหนด
- หากบัญชีใดที่ไม่มีการล็อกอินเกิน 45 วันให้ระงับการใช้งานบัญชีนั้นโดยอัตโนมัติ
- พัฒนาระบบให้รองรับการใช้งานร่วมกับโปรแกรมบริหารจัดการพาสเวิร์ด รวมถึงอนุญาตให้ช่องกรอกพาสเวิร์ดนั้นสามารถ Paste ข้อมูลได้

รู้ทัน ป้องกันอีเมล

1 ตั้ง **Password** ที่คาดเดาได้ยาก

2 ดูแลช่องทางที่ใช้ในการ **Reset พาสเวิร์ด** ให้มีความมั่นคงปลอดภัย
เช่น อีเมลสำรองสำหรับกู้คืนบัญชี

3 ตรวจสอบประวัติ การใช้งานที่น่าสงสัย รวมถึงช่องทางใน **การยืนยันตัวตน** อย่างสม่ำเสมอ

4 ติดตั้งโปรแกรม **แอนติไวรัส**
อัปเดตระบบปฏิบัติการ เบราว์เซอร์ และซอฟต์แวร์ ให้ทันสมัย

5 หลีกเลี่ยงการใช้เว็บเมล ผ่านเครื่องคอมพิวเตอร์สาธารณะ และไม่ควรตั้งค่าให้จำพาสเวิร์ด

6 ระมัดระวัง **อีเมลที่มีไฟล์แนบ** หรือลิงก์พาไปเว็บไซต์อื่น

7 แม้อีเมลจากคนที่รู้จัก **ก็อาจจะเป็นคนร้าย** แปลงแปลงมาก็ได้ หากไม่แน่ใจ **ควรยืนยัน ผ่านช่องทางอื่นที่ไม่ใช่อีเมล**
เช่น แจ้งยืนยันเปลี่ยนเลขที่บัญชีโอนเงินทางโทรศัพท์

8 ON เปิดการใช้งานยืนยันตัวตนแบบ **Multi-Factor Authentication**
โดยใช้ OTP หรือ Pin ในการยืนยันตัวตน

9 เช็กรายชื่อผู้จะได้รับอีเมล **ก่อนกดปุ่ม Reply หรือ Reply All ทุกครั้ง**
ผู้ร้ายมักใช้เทคนิคตั้งชื่ออีเมล **ที่ใกล้เคียงกับคนที่เรารู้จัก**
เช่น somsak@yahoo.com vs. somsak@yah00.com
(เลขศูนย์แทนอักษร o)

10 อย่าหลงเชื่ออีเมลที่หลอกให้เปลี่ยน **Password** หรือให้อัปเดตข้อมูลส่วนตัว
หากไม่แน่ใจควรสอบถามกับผู้ที่ส่งข้อมูลมาในช่องทางอื่น ๆ อีกครั้ง

10 คำแนะนำป้องกัน **คุกคามทาง Email**

GO DIGITAL with ETDA

อีเมลถือเป็นทรัพย์สินสำคัญที่ต้องมีมาตรการรักษาความมั่นคงปลอดภัย

เพราะถ้าถูกผู้ไม่หวังดีเข้าถึงหรือยึดอีเมลได้ ก็จะใช้แอบอ้างเพื่อทำธุรกรรมต่าง ๆ แทนเรา สร้างความเสียหายทั้งเงินและชื่อเสียงอีกด้วย ดังนั้น เราควร

1. ตั้งพาสเวิร์ด ที่ไม่ซ้ำ ไม่ง่าย และไม่บอกใคร
2. ตั้งค่าหรือปรับปรุงข้อมูลระบุตัวตนให้ทันสมัย และตรงกับความเป็นจริง เช่น อีเมลสำรองสำหรับกู้คืนบัญชี
3. ตรวจสอบประวัติการใช้งานที่น่าสงสัย รวมถึงช่องทางในการยืนยันตัวตนอย่างสม่ำเสมอ
4. ติดตั้งโปรแกรมแอนติไวรัส อัปเดตระบบปฏิบัติการ เบราว์เซอร์ และซอฟต์แวร์ให้ทันสมัย
5. ไม่ติดตั้งโปรแกรมจากแหล่งที่ไม่รู้จัก ไม่ใช้โปรแกรมเถื่อน
6. ระมัดระวังอีเมลที่มีไฟล์แนบ หรือลิงก์ที่พาไปเว็บไซต์อื่น
7. ยืนยันการเปลี่ยนเลขบัญชีผ่านช่องทางอื่นที่ไม่ใช่อีเมล
8. เปิดการใช้งานยืนยันตัวตนแบบ Multi-Factor Authentication
9. เช็กรายชื่อผู้จะได้รับอีเมล ก่อนกดปุ่ม Reply หรือ Reply All ทุกครั้ง
10. อย่าหลงเชื่ออีเมลที่หลอกให้เปลี่ยนพาสเวิร์ดหรือให้อัปเดตข้อมูลส่วนบุคคล หากไม่แน่ใจว่าเป็นอีเมลที่มาจากใคร ให้รีบปรึกษาผู้เชี่ยวชาญด้านไอที หรือสอบถามกับผู้ที่ส่งข้อมูลมาในช่องทางอื่น ๆ กลับไปอีกครั้ง เพื่อยืนยันว่าความถูกต้องก่อนดำเนินการใด ๆ

รู้ทัน ป้องกันการใช้มือถือ

แค่มือถือหาย อาจจะร้ายกว่าที่คิด

ข้อมูล ส่วนตัวหรือความลับองค์กร
ที่ไม่อยากให้โลกรู้จะหลุดออกไป
แถมอาจ ถูกข่มขู่ เรียกค่าไถ่

ถูก สะกดรอย
และสวมรอยการใช้งาน
จากบริการต่าง ๆ
เพื่อทำความผิด

ข้อมูลสำคัญ อาจหาย
แถม กู้คืนไม่ได้

กันไว้ เหอะ ดีกว่าแก้

- ต้องรู้ก่อนว่าเราเก็บข้อมูล หรือ APPLICATION อะไรในมือถือบ้าง
- ตั้งรหัสล็อกหน้าจอมือถือ และ PASSWORD ในการเข้า APPLICATION ต่าง ๆ เหมือนใส่ ล็อก 2 ชั้น
- LOGOUT เสมอ เมื่อไม่ใช้ APPLICATION
- ไม่บันทึกข้อมูล USERNAME และ PASSWORD ไว้ในมือถือ
- แอนดรอยด์ ให้เปิดใช้ FIND MY DEVICE
- iOS ให้เปิดใช้ FIND MY IPHONE

จากในมือถือ ซึ่งเป็นระบบที่สามารถ
ล็อกหรือล้างข้อมูลมือถือ
จากเบราว์เซอร์ เมื่อมือถือหายได้

ถ้าหาย แล้ว ทำไงดี

- แจ้งผู้ให้บริการ APPLICATION เพื่อ ระงับการให้บริการ เช่น e-BANKING
- เปลี่ยน PASSWORD ในการเข้าใช้บริการต่าง ๆ ที่มีในมือถือ
- แจ้งความกับตำรวจ เพื่อหาตัวผู้ร้าย และเพื่อเป็นหลักฐาน กรณีผู้ร้ายอาจนำมือถือไปทำความผิดต่อภายหลัง
- FIND MY DEVICE LOGIN ด้วยอีเมลของ GOOGLE ส่วน FIND MY IPHONE – ICLOUD LOGIN ด้วยบัญชีเดียวกับมือถือ จากนั้นจะสามารถควบคุมให้มือถือล็อกและล้างข้อมูลได้

GO DIGITAL with ETDA

แค่มือถือหาย อาจจะร้ายกว่าที่คิด!

- เมื่อมือถือสูญหายหรือถูกขโมยข้อมูลที่ไม่อยากเปิดเผย หรือข้อมูลองค์กรที่เก็บไว้ในโทรศัพท์อาจจะหลุดออกไป และมีความเสี่ยงที่ข้อมูลไม่สามารถกู้คืนได้
- ถูกนำข้อมูลไปเผยแพร่ เพื่อข่มขู่ เรียกค่าไถ่
- ถูกสะกดรอยการใช้งานจากบริการต่าง ๆ
- ถูกแอบอ้างสวมรอยใช้งานเพื่อกระทำความผิด

คำแนะนำในการใช้มือถือ

- ต้องรู้ก่อนว่าเราเก็บข้อมูล หรือมีโปรแกรมอะไรในมือถือบ้างเพื่อป้องกันข้อมูลอื่น ๆ ของเราที่เชื่อมกับอุปกรณ์อื่น เพื่อหยุดการเชื่อมต่อกับมือถือได้ เช่น ข้อมูลการเงินผ่านการใช้แอปของธนาคาร หรือโปรแกรมกล้องวงจรปิดที่เชื่อมต่อกับมือถือ
- ตั้งรหัสล็อกหน้าจอมือถือ และใส่พาสเวิร์ดในการเข้าโปรแกรมต่าง ๆ ในมือถือ เช่น Line ที่สามารถตั้งค่าก่อนเข้าใช้งานได้ เหมือนใส่ล็อก 2 ชั้น
- เมื่อใช้งานโปรแกรม หรือแอปแล้ว ควร Logout เสมอ
- ไม่บันทึกข้อมูล Username และพาสเวิร์ด ไว้ในมือถือ
- ข้อมูลสำคัญ ๆ หรือข้อมูลส่วนตัว เมื่อใช้งานเสร็จแล้วควรลบทิ้ง

เมื่อมือถือหายให้ตั้งสติ และดำเนินการตามขั้นตอน ดังนี้

- แจ้งผู้ให้บริการแอปพลิเคชัน เพื่อระงับการให้บริการ เช่น e-Banking
- เปลี่ยน Username และพาสเวิร์ดในการเข้าใช้บริการต่าง ๆ ที่มีในมือถือ
- แจ้งความกับตำรวจเพื่อหาตัวผู้ร้าย และเพื่อเป็นหลักฐานกรณีผู้ร้ายอาจนำมือถือกระทำความผิดต่อภายหลัง
- เข้าโปรแกรมของมือถือ เช่น Find My iPhone หรือ Find My Device เพื่อค้นหา บล็อกการเข้าถึง หรือลบข้อมูลในมือถือจากระยะไกล

รู้ทัน ป้องกันภัย
โซเชียลมีเดีย

1 คิดให้รอบ
สักนิดก่อนโพสต์

เพราะมันเปิดเผยและทุกคนเข้าถึงได้ง่าย
การโพสต์ข้อมูลที่สุ่มเสี่ยงจึงอาจเป็นภัยต่อตัวเอง

2 ระมัดระวัง
ในการคลิกลิงก์

ที่มากับการแชร์ เพราะอาจนำไปสู่ไวรัส
หรือช่องทางขโมยข้อมูลของเหล่าแฮกเกอร์

3
เข้าโซเชียลเน็ตเวิร์ก
พิมพ์ URL โดยตรง

เลี่ยงคลิกลิงก์ เพราะอาจเป็น URL ปลอม
หลอกเอาบัญชีใช้งานของเราเช่น facebook.com
อาจมี URL หลอกเป็น faeebook.com

4 รอบคอบ
ก่อนตอบรับเป็นเพื่อน

คัดกรองคนที่ขอเป็นเพื่อนโดยเข้าไปดูโปรไฟล์
ก่อนทุกครั้งเพราะอาจมีผู้ไม่หวังดีแฝงมาด้วย

5 ตั้งค่า
ความเป็นส่วนตัว

หลีกเลี่ยงตั้งค่าแบบสาธารณะและอนุญาตให้เพื่อน
เท่านั้นที่เห็นกิจกรรมของเราได้

6 ไม่แสดงข้อมูล
ส่วนตัวที่เป็นความลับ

เช่น บัตรประชาชน บัตรเครดิต ไม่ว่าจะอยู่ในรูปแบบ
ข้อความหรือรูปภาพก็ตาม

7
เปิดใช้งาน
Do Not Track

ป้องกันการติดตามและเก็บข้อมูลจากผู้ให้
บริการโซเชียลเน็ตเวิร์กรวมถึงผู้ไม่หวังดี
ที่เข้ามาขโมยข้อมูล

8 ใช้วิจารณญาณ
ในการรับข่าวสาร

อย่าปักใจเชื่อก่อนที่ อาจมีการสร้างกระแส สวมรอย
สมอ้างจากผู้ไม่หวังดี

9 ควบคุมการใช้งาน
ของบุตรหลาน

ลองหาเครื่องมือมาเป็นตัวช่วย
เช่น Windows Live Family Safety

10
ตระหนักว่าเป็น
สังคมเสรี

แม้ทุกคนมีสิทธิ์ในการแสดงความเห็น
แต่การกระทำที่ไม่เหมาะสมก็เป็นเหตุให้ถูกฟ้องร้อง
และศาลก็อาจรับฟังคำร้องด้วย

GO DIGITAL with ETDA

ในยุคที่โซเชียลมีเดียมีการใช้งานอย่างแพร่หลายในการแสดงออกทางความคิด เผยแพร่ข้อมูลข่าวสาร รวมถึงทำธุรกิจออนไลน์ ซึ่งมีประโยชน์และสะดวกสบาย แต่มีด้านดีก็ต้องมีด้านร้าย เช่น การแชร์ข้อมูลที่ทำได้ง่าย ทำให้ผู้ใช้ไม่ได้ตรวจสอบความถูกต้องและแชร์ข้อมูลที่ผิดพลาดการแชร์ข้อมูลส่วนตัวเกินความจำเป็น หรือผู้ไม่หวังดีอาจใช้โซเชียลมีเดียเป็นช่องทางในการหลอกลวงต่าง ๆ ผู้ใช้จึงควรรู้จักหลีกเลี่ยงการใช้งานโซเชียลมีเดียในทางที่ไม่เหมาะสม ซึ่งอาจส่งผลร้ายต่อทั้งตัวเองและผู้อื่น ดังนี้

1. คิดให้รอบคอบก่อนโพสต์ข้อมูลใด ๆ
2. ใช้ความระมัดระวังในการคลิกลิงก์ต่าง ๆ เพราะอาจเป็นลิงก์ที่ทำให้ติดมัลแวร์และถูกขโมยข้อมูลได้
3. พิมพ์ที่อยู่ URL ของเว็บไซต์โซเชียลเน็ตเวิร์กนั้น ๆ โดยตรง เพื่อหลีกเลี่ยงการเข้าเว็บไซต์ปลอมที่หลอกขโมยรหัสผ่าน
4. คัดกรองคนที่ขอเป็นเพื่อน หลีกเลี่ยงการตอบรับคนที่ไม่รู้จักกันมาก่อน
5. ตั้งค่าความเป็นส่วนตัว เพื่อป้องกันไม่ให้ข้อมูลหลุดออกไปยังผู้ไม่หวังดี
6. ไม่แสดงข้อมูลส่วนตัวที่เป็นความลับ เช่น หมายเลขบัตรประชาชน, หมายเลขบัตรเครดิต
7. เปิดใช้งานคุณสมบัติ Do Not Track ของเบราว์เซอร์ เพื่อป้องกันการติดตามและการเก็บข้อมูลของผู้ให้บริการ
8. ใช้วิจารณญาณในการรับข่าวสาร และอย่าปักใจเชื่อข้อมูลที่เผยแพร่เข้ามาในทันที
9. ดูแลและควบคุมการใช้งานของบุตรหลานอย่างใกล้ชิด สอนให้บุตรหลานรู้จักวิเคราะห์ข้อมูล และรู้จักเล่นอย่างถูกวิธี
10. ตระหนักว่าถึงแม้ว่าจะสามารถแสดงความคิดเห็นได้ แต่การพาดพิงบุคคลที่สาม หรือการกระทำที่ไม่เหมาะสมก็อาจเป็นเหตุให้ถูกดำเนินคดีตามกฎหมายได้

รู้ทัน
ป้องกันซื้อของออนไลน์

แนวทางแก้ไขเมื่อเจอปัญหาซื้อขายออนไลน์

ถูกลักลอบ/โจรกรรมข้อมูลบัตรเครดิตระหว่างชำระเงินออนไลน์

1 

ติดต่อธนาคารเจ้าของบัตรเพื่อระงับการใช้

2 

ทำลายบัตรเก่าทิ้ง

เน้นทำลายแถบแม่เหล็กและชิปบันทึกข้อมูลบนบัตร

3 

ตรวจสอบกับทางธนาคารถึงการคืนเงิน

ว่าสามารถทำได้หรือไม่ และต้องใช้หลักฐานอย่างไรในการยืนยันว่าการทำธุรกรรมซื้อขายที่เป็นปัญหานั้นไม่ได้เกิดจากความตั้งใจของเราจริง ๆ

4 

ลบข้อมูลบัตรเครดิต

ที่เคยบันทึกไว้บนเว็บไซต์หรือระบบต่าง ๆ ที่ช่วยในการซื้อของออนไลน์เพื่อเป็นการทำลายข้อมูลทั้งหมด

เกิดข้อพิพาทระหว่างผู้ซื้อและผู้ขาย กรณีปัญหาไม่ใหญ่

เช่น สินค้าที่ไม่ได้คุณภาพ สินค้าแตกหัก หรือได้รับสินค้าไม่ครบ

1 

อ่านข้อกำหนดบนเว็บไซต์ที่ขายสินค้า

ว่ามีนโยบายการคืนสินค้า หรือแก้ปัญหาเหล่านี้หรือไม่

2 

หากชี้แจงไว้ก็ให้ทำตามเพื่อแก้ปัญหา

3 

แต่ถ้าหากไม่ได้ชี้แจง

ควรติดต่อผู้ขายและเจรจาเพื่อแก้ปัญหาที่เกิดขึ้น ซึ่งผู้ขายอาจรับผิดชอบโดยการคืนเงิน การเปลี่ยนสินค้า

เกิดข้อพิพาทเป็นการทำผิดโดยตั้งใจของผู้ขาย

เช่น ผู้ซื้อจ่ายเงินแล้วแต่ผู้ขายไม่ส่งสินค้ามาให้ แสดงถึงเจตนาไม่ดีของผู้ขาย

1 

รวบรวมเอกสารทุกอย่าง

ที่เกิดขึ้นในการซื้อสินค้าออนไลน์

2 

เข้าแจ้งความกับตำรวจ

เป็นความผิดฐานฉ้อโกงประชาชน และรับใบแจ้งความกลับมา

3 

อาจสืบหาข้อมูลเพิ่มเติมของร้านค้า/ผู้ขาย

จากเลขที่บัญชี พร้อมใบแจ้งความและหลักฐานการโอนเงินไปยังธนาคาร แล้วทำเรื่องขอรายละเอียดของเจ้าของบัญชีดังกล่าว

4 

ติดตามความคืบหน้าจากหน่วยงานที่ร้องเรียน หรือแจ้งเรื่องร้องเรียนไปที่ 1212 OCC

หรือหน่วยงานด้านการคุ้มครองผู้บริโภค เช่น สคบ. สายด่วน 1166 อย. สายด่วน 1556

GO DIGITAL with ETDA

คนซื้อดูให้มั่นใจ ถ้าพลั้งผิดมีทางออก

- พ่อค้าแม่ค่าน่าเชื่อถือไหม ต้องตรวจสอบ โดยดูจากที่อยู่ เบอร์โทรศัพท์ หรือตรวจสอบไปถึงการจดทะเบียนการค้า ตรวจสอบประวัติของผู้ขายและเลขที่บัญชีโดยสืบค้นใน google ว่ามีประวัติไม่ดี หรือเคยถูกร้องเรียนมาก่อนหรือไม่ และยังเช็กจากรีวิวของผู้ซื้อรายอื่น ๆ ได้อีกทาง
- หากมีหน้าร้านจริง ๆ ด้วย ก็จะลดความเสี่ยงลงได้ การซื้อของจากร้านค้าที่ขายบนแพลตฟอร์มที่น่าเชื่อถือ ก็เป็นอีกทางเลือกที่น่าไว้ใจได้
- ควรตรวจสอบเงื่อนไขของสินค้า การรับประกัน ว่ามีหรือไม่ อย่างไร การส่งคืนสินค้าหากไม่เป็นไปตามที่สั่งซื้อ ใครเป็นคนรับผิดชอบค่าใช้จ่ายในการส่ง-คืนสินค้า การหักค่าใช้จ่ายหรือค่าบริการต่าง ๆ
- สงสัยไว้ก่อน การซื้อสินค้าจากร้านค้าหรือผู้ขายที่ขายของราคาต่ำกว่าปกติมาก ๆ อาจเสี่ยงกับการถูกหลอกลวง ไม่ได้รับสินค้า หรือได้สินค้าไม่มีคุณภาพ
- ไม่แจ้งเลขบัตรเครดิต เลขบัตรประจำตัวประชาชน ข้อมูลส่วนตัวอื่น ๆ เช่น ที่อยู่ อีเมล เบอร์โทรศัพท์ส่วนตัว ลงบนพื้นที่ออนไลน์สาธารณะ

กรณีซื้อขายมีปัญหาทำไงดี

1. เก็บหลักฐานต่าง ๆ เช่น รูปและชื่อโปรไฟล์ของร้านค้าหรือผู้ขาย หน้าประกาศขายสินค้า หากเป็นเว็บไซต์ให้เก็บ URL (ที่อยู่เว็บไซต์) ชื่อ ที่อยู่ เบอร์โทรศัพท์ของร้านค้าหรือผู้ขาย เลขที่บัญชีของผู้ขายที่ให้โอนเงินชำระค่าสินค้า ภาพหน้าจอข้อความพูดคุยที่แสดงถึงการตกลงซื้อขาย เช่น ภาพตัวอย่างสินค้า ข้อความโฆษณา ราคาสินค้า การต่อรอง การรับประกัน การโอนเงินต่าง ๆ ไม่ว่าจะทางอีเมล ข้อความส่วนตัว ไลน์ หรือช่องทางอื่น ๆ หลักฐานการโอนเงินค่าสินค้า

2. นำหลักฐานตามข้อ 1 พร้อมทั้งสมุดบัญชีธนาคารและบัตรประจำตัวประชาชนไปแจ้งความที่สถานีตำรวจใกล้บ้าน โดยระบุขอให้ดำเนินคดีให้ถึงที่สุด

3. อาจสืบหาข้อมูลเพิ่มเติมของร้านค้า/ผู้ขาย จากเลขที่บัญชี โดยนำเลขที่บัญชีของร้านค้าหรือผู้ขาย พร้อมใบแจ้งความและหลักฐานการโอนเงินไปยังธนาคาร แล้วทำเรื่องขอรายละเอียดของเจ้าของบัญชีดังกล่าว ยื่นเรื่องขอเงินคืน หรืออายัดบัญชี แต่บางครั้ง เลขที่บัญชีที่โอนเงินค่าสินค้าไปให้ อาจจะไม่ใช่ของมิจฉาชีพที่แท้จริง เพราะเจ้าของบัญชีอาจโดนนำบัตรประชาชนไปสวมรอยเปิดบัญชีหลอกขายสินค้า ก็เป็นไปได้เช่นกัน อีกประการหนึ่งคนร้ายมักจะรีบถอนเงินออกไปทันที ทำให้มักไม่ได้เงินคืนจากธนาคาร

4. หรือขอคำปรึกษา แจ้งเรื่องร้องเรียน พร้อมส่งหลักฐานตามข้างต้น ได้ที่ ศูนย์รับเรื่องร้องเรียนปัญหาออนไลน์ 1212 Online Complaint Center หรือ 1212 OCC ผ่านสายด่วน 1212 ตลอด 24 ชม.

รู้ทัน ป้องกันมัลแวร์

มัลแวร์ เป็นโปรแกรมที่ถูกพัฒนาขึ้นเพื่อส่งให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ เช่น การขโมยข้อมูล การสอดแนมดูพฤติกรรมการใช้งาน และการใช้เป็นฐานโจมตีระบบอื่น

สถานการณ์สมมุติ

4 เทคนิค วัคซีนป้องกัน มัลแวร์

1. **ไม่คลิกลิงก์** หรือเปิดไฟล์ในอีเมลที่น่าสงสัย ถ้าไม่ไว้ใจควรถามจากผู้ส่งโดยตรง
2. **ติดตั้ง/อัปเดต Antivirus** และหมั่นอัปเดตระบบปฏิบัติการ
3. **Backup** ข้อมูลอยู่เสมอ (ถ้าเป็นไปได้ให้เก็บข้อมูล Backup ในอุปกรณ์ที่ไม่ได้เชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ)
4. ถ้ามีการแชร์ข้อมูลร่วมกันผ่านระบบเครือข่าย **ให้ตรวจสอบสิทธิ์เข้าถึงข้อมูล** และ **กำหนดสิทธิ์ให้ผู้ใช้** มีสิทธิ์เฉพาะไฟล์ที่จำเป็น

GO DIGITAL with ETDA

มัลแวร์ (Malware) หรือ Malicious Code เป็นโปรแกรมที่ถูกพัฒนาขึ้น เพื่อให้เกิดผลลัพธ์ที่ไม่พึงประสงค์กับผู้ใช้งานหรือระบบ เช่น ทำให้เกิดความขัดข้อง หรือเสียหายกับระบบที่โปรแกรมดังกล่าวติดตั้งอยู่ โดยปกติภัยคุกคามประเภทนี้ ต้องอาศัยการหลอกลวงให้ผู้ใช้งานเรียกใช้งานโปรแกรมก่อนจึงจะสามารถทำการโจมตีได้ เช่น Virus, Trojan หรือ Spyware ต่าง ๆ หรือบางครั้งอาจทำการโจมตีได้ด้วยตนเอง เช่น Worm

4 ข้อเบื้องต้น ป้องกันมัลแวร์

1. ไม่คลิกลิงก์ หรือเปิดไฟล์อีเมลที่น่าสงสัย ถ้าไม่ไว้ใจควรถามจากผู้ส่งโดยตรง
2. ติดตั้งและอัปเดตแอนติไวรัส และหมั่นอัปเดตระบบปฏิบัติการ
3. แบ็กอัปข้อมูลอยู่เสมอ หากเป็นไปได้ให้เก็บข้อมูลในอุปกรณ์ที่ไม่ได้เชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ
4. หากมีการแชร์ข้อมูลร่วมกันผ่านระบบเครือข่าย ให้ตรวจสอบสิทธิ์เข้าถึงข้อมูล และกำหนดสิทธิ์ให้ผู้ใช้มีสิทธิ์เฉพาะไฟล์ที่จำเป็นเท่านั้น

รู้ทัน
ป้องกันแรนซัมแวร์

รูปแบบการโจมตีของ Ransomware
เพื่อยึดข้อมูลในเครื่องคอมพิวเตอร์ของเหยื่อ

ข้อแนะนำในการป้องกันความเสียหายจากภัย Ransomware

ดำเนินการทันทีเพื่อรักษาความพร้อมใช้งานของข้อมูล

สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอ

ติดตั้ง/อัปเดตโปรแกรมป้องกันไวรัส (Antivirus) รวมถึงอัปเดตโปรแกรมอื่น ๆ

มีความตระหนักในการใช้อีเมลและเปิดเว็บไซต์

ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าส

ดาวน์โหลดซอฟต์แวร์จากแหล่งที่น่าเชื่อถือเท่านั้น

ในกรณีที่ตกเป็นเหยื่อ

ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อและอุปกรณ์เก็บข้อมูลเคลื่อนที่

ให้ติดต่อผู้เชี่ยวชาญ หรือ ไทยเซิร์ต ทันที

GO DIGITAL with ETDA

มัลแวร์หรือโปรแกรมประสงค์ร้ายที่เรียกว่า แรนซัมแวร์ (Ransomware) หรือมัลแวร์เรียกค่าไถ่ จะเกิดเหตุขึ้นเมื่อเปิดไฟล์แนบ โดยมัลแวร์นี้จะโจมตีด้วยวิธีการเข้ารหัสลับ (Encryption) ไฟล์เอกสารต่าง ๆ บนเครื่องที่ติดมัลแวร์ รวมถึงเอกสารที่แชร์ผ่านเครือข่ายและจากอุปกรณ์ External Drive ที่เสียบอยู่กับเครื่องคอมพิวเตอร์ ซึ่งไฟล์ของเครื่องเหยื่อจะยังอยู่ แต่ไม่สามารถเปิดอ่านข้อมูลได้ จนกว่าจะจ่ายเงินเพื่อเป็นค่าใช้จ่ายในการส่งรหัสสำหรับถอดรหัสลับข้อมูล (Decryption) กลับมา หากแต่ในความเป็นจริงมีหลายกรณีที่พบว่าการจ่ายเงินค่าไถ่ไปแล้ว เหยื่อกลับไม่ได้ข้อมูลคืนมาอย่างที่อ้างไว้ซึ่งส่งผลเสียหายทั้งในระดับบุคคล บริษัทหรือองค์กรโดยเฉพาะการสูญเสียข้อมูลสำคัญของบริษัทหรือองค์กร การตระหนักถึงอันตรายและการป้องกันแรมซัมแวร์จึงเป็นมาตรการที่มีประสิทธิภาพในการลดผลกระทบมากกว่าการแก้ไข

วิธีการป้องกันด้วยตัวเอง เพื่อไม่ให้ตกเป็นเหยื่อภัยคุกคามดังกล่าวคือ

1. สำรองข้อมูลสำคัญที่ใช้งานอย่างสม่ำเสมอและหากเป็นไปได้ให้เก็บข้อมูลที่ทำการสำรองไว้ในอุปกรณ์ที่ไม่มีการเชื่อมต่อกับคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ
2. อัปเดตโปรแกรมแอนติไวรัส รวมถึงโปรแกรมอื่น ๆ โดยเฉพาะโปรแกรมที่มักมีปัญหาเรื่องช่องโหว่อยู่บ่อย ๆ
3. ไม่คลิกลิงก์หรือเปิดไฟล์ที่มาพร้อมกับอีเมลที่น่าสงสัยหากไม่มั่นใจว่าเป็นอีเมลที่น่าเชื่อถือหรือไม่เคยรู้จักมาก่อน
4. ดาวน์โหลดซอฟต์แวร์ที่น่าเชื่อถือเท่านั้น เพราะผู้ร้ายอาจฝังมัลแวร์ในซอฟต์แวร์ที่เปิดดาวน์โหลดได้ฟรี

สำหรับกรณีที่ผู้ใช้งานอีเมลตกเป็นเหยื่อมัลแวร์เรียกค่าไถ่ ให้รีบดำเนินการ

1. ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อ กับระบบเครือข่ายคอมพิวเตอร์ขององค์กรและเครือข่ายอินเทอร์เน็ตในทันที
2. ตัดการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อกับอุปกรณ์เก็บข้อมูลเคลื่อนที่ (Portable Storage) หรือระบบเก็บข้อมูลบนเครือข่าย (Network Storage) ทุกประเภท หลังการตัดการเชื่อมต่อข้างต้น ให้ติดต่อกับผู้เชี่ยวชาญด้าน IT ทันทีหรือขอคำปรึกษาได้ที่ไทยเซิร์ต ทางอีเมล report@thaicert.or.th หรือโทรศัพท์ 0 2123 1212

แนวทาง รับมือมัลแวร์เรียกค่าไถ่ ransomware สำหรับหน่วยงานของรัฐ

มาตรการพื้นฐานสำหรับเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ กรณีมัลแวร์เรียกค่าไถ่ สำหรับหน่วยงานของรัฐ

1. **จัดทำหรือทบทวนแนวนโยบาย**และแนวปฏิบัติงาน
2. **สำรองข้อมูลที่สำคัญ**
3. **ควบคุมการเข้าถึงเครือข่าย** และระบบสารสนเทศ
4. **ประเมินความเสี่ยง**ด้านระบบสารสนเทศ
5. จัดเก็บ**บันทึกกิจกรรม (Log) ไปยังพื้นที่จัดเก็บในส่วนกลาง**
6. ทบทวน และ**ยกเลิกบริการที่ไม่จำเป็นบนเครื่องให้บริการ**
7. **กำหนดเจ้าหน้าที่ประสานงาน**ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับบริหารกับระดับปฏิบัติการ
8. ให้ความรู้กับผู้ใช้งานในหน่วยงานเกี่ยวกับการป้องกันตนเองจากการติดมัลแวร์เรียกค่าไถ่

แนวทางการดำเนินการรับมือสถานการณ์ กรณีหน่วยงานของรัฐพบความเสียหายที่เกิดขึ้นจากมัลแวร์เรียกค่าไถ่

1. ตัดการเชื่อมต่อทางเครือข่าย
2. สำรองข้อมูลที่ยังใช้งานได้อยู่จากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์

หากพบความเสียหาย ที่เกิดขึ้นจากมัลแวร์เรียกค่าไถ่

- แจ้งเหตุไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และไทยเซิร์ต (ทางอีเมล report@thaicert.or.th)
- เปลี่ยนรหัสผ่านที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงรหัสผ่านที่ใช้งานผ่านระบบควบคุมบัญชีผู้ใช้งานทั้งหมด
- ตรวจสอบสายพันธุ์ของมัลแวร์เรียกค่าไถ่โดยอาศัยข้อมูลที่ปรากฏในเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ เช่น นามสกุลของไฟล์ที่เปลี่ยนไป ข้อความที่ปรากฏบนหน้าจอ เพื่อประเมินวิธีการแก้ไขปัญหา เช่น การกู้คืนข้อมูล
- หากประสงค์ใช้เครื่องมือถอดรหัสลับข้อมูล ควรทำในสภาพแวดล้อมที่ไม่มีการเชื่อมต่อทางเครือข่าย เพื่อลดความเสี่ยงที่อาจเกิดจากการใช้เครื่องมือดังกล่าว

อ่านรายละเอียดเพิ่มเติมที่นี่

GO DIGITAL with ETDA

แนวทางรับมือมัลแวร์เรียกค่าไถ่สำหรับหน่วยงานของรัฐ

มาตรการพื้นฐานสำหรับเตรียมความพร้อม

1. จัดทำหรือทบทวนแนวนโยบายและแนวปฏิบัติงาน
2. สำรองข้อมูลที่สำคัญ
3. ควบคุมการเข้าถึงเครือข่าย และระบบสารสนเทศ
4. ประเมินความเสี่ยงด้านระบบสารสนเทศ
5. จัดเก็บบันทึกกิจกรรม (Log) ไปยังพื้นที่จัดเก็บในส่วนกลาง
6. ทบทวน และยกเลิกบริการที่ไม่จำเป็นบนเครื่องให้บริการ
7. กำหนดเจ้าหน้าที่ประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับบริหารกับระดับปฏิบัติการ
8. ให้ความรู้กับผู้ใช้งานในหน่วยงานเกี่ยวกับการป้องกันตนเองจากการติดมัลแวร์เรียกค่าไถ่

แนวทางการดำเนินการรับมือสถานการณ์กรณีพบความเสียหาย

1. ตัดการเชื่อมต่อทางเครือข่าย
2. สำรองข้อมูลที่ยังใช้งานได้อยู่จากเครื่องคอมพิวเตอร์ที่ติดมัลแวร์หากพบความเสียหายที่เกิดขึ้นจากมัลแวร์เรียกค่าไถ่

หากพบความเสียหายที่เกิดจากมัลเวร์เรียกค่าไถ่

- แจ้งเหตุไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และไทยเซิร์ต (ทางอีเมล report@thaicert.or.th)
- เปลี่ยนรหัสผ่านที่เกี่ยวข้องกับเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ รวมถึงรหัสผ่านที่ใช้งานผ่านระบบควบคุมบัญชีผู้ใช้งานทั้งหมด
- ตรวจสอบสายพันธุ์ของมัลแวร์เรียกค่าไถ่โดยอาศัยข้อมูลที่ปรากฏในเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ เช่น นามสกุลของไฟล์ที่เปลี่ยนไป ข้อความที่ปรากฏบนหน้าจอ เพื่อประเมินวิธีการแก้ไขปัญหา เช่น การกู้คืนข้อมูล
- หากประสงค์ใช้เครื่องมือถอดรหัสลับข้อมูล ควรทำในสภาพแวดล้อมที่ไม่มีการเชื่อมต่อทางเครือข่าย เพื่อลดความเสี่ยงที่อาจเกิดจากการใช้เครื่องมือดังกล่าว

แบ็กอัปข้อมูลไว้ก่อน
เพราะถ้าหายไป เสียเงินเท่าไร...
ก็อาจไม่ได้คืนมา

สำหรับ SMEs

รู้มั้ย? **363%**
คือสถิติที่เพิ่มขึ้นช่วง Q2 ปี 61 - Q2 ปี 62

การโจมตีภาคธุรกิจด้วยมัลแวร์เรียกค่าไถ่

ซึ่งจะล็อกข้อมูลในเครื่อง เช่น เอกสาร รูปภาพ ทำให้เปิดใช้งานไม่ได้เพื่อเรียกค่าไถ่
และแม้จ่ายค่าไถ่ไปแล้ว**ก็ไม่ได้รับประกัน**ว่าจะได้ข้อมูลนั้นคืนมา

แบ็กอัปแบบไหน...ถามใจเธอดู?

วิธีเก็บ	ข้อดี	ข้อเสีย
บริการ Cloud เช่น Google Drive, Dropbox, OneDrive	ใช้ง่าย ฟรี เข้าที่ไหนก็ได้ แบ็กอัปอัตโนมัติได้	ต้องมีอินเทอร์เน็ต มีความเสี่ยงปิดบริการ
อุปกรณ์เก็บข้อมูลแบบพกพา เช่น DVD, ฮาร์ดดิสก์, Flash Drive	ใช้ง่าย เก็บรักษาในที่ปลอดภัย พกติดตัวได้	มีโอกาสสูญหายหรือเสียหาย
พิมพ์เป็นกระดาษ	ไม่ขึ้นต่อฮาร์ดแวร์ ป้องกันการถูกเจาะข้อมูล	จัดการยาก ไม่ดีต่อสิ่งแวดล้อม
NAS (Network-attached storage)	เก็บข้อมูลจากคอมพิวเตอร์หลายเครื่อง พร้อมกันได้ แบ็กอัปอัตโนมัติได้	ต้องติดตั้งและดูแลระบบ ราคาสูง มีโอกาสเสียหาย

(1) : https://www.thaicert.or.th/newsbite/2019-08-15-01.html

NAS (Network-attached storage)
*คือ อุปกรณ์ที่ให้บริการเก็บและแชร์ข้อมูลแก่เครื่องของผู้ใช้งานในเครือข่ายเดียวกัน

ข้อมูลเพิ่มเติม ศึกษาได้ที่
www.thaicert.or.th / www.etda.or.th

GO DIGITAL with ETDA

ข้อแนะนำการแบ็กอัปข้อมูลสำหรับภาคธุรกิจ เพื่อป้องกันมัลแวร์เรียกค่าไถ่

มัลแวร์เรียกค่าไถ่ เป็นซอฟต์แวร์ที่มีจุดประสงค์เพื่อสร้างความเสียหาย โดยจะเข้ารหัสลับไฟล์ข้อมูลภายในเครื่องเพื่อไม่ให้สามารถใช้งานข้อมูลนั้น ๆ ได้ จากนั้นจะเรียกร้องให้จ่ายเงินค่าไถ่เพื่อแลกกับการได้กุญแจถอดรหัสลับข้อมูลกลับคืนซึ่งอาจไม่สามารถยืนยันได้ว่าหากจ่ายเงินแล้วจะกู้คืนข้อมูลได้จริงตามที่อ้าง

จากรายงานของบริษัท Malwarebytes สถิติตั้งแต่ไตรมาสที่สองของปี 2561 จนถึงไตรมาสที่สองของปี 2562 พบมัลแวร์เรียกค่าไถ่โจมตีหน่วยงานภาคธุรกิจเพิ่มขึ้นกว่า 363% ในขณะที่การโจมตีผู้ใช้งานทั่วไปพบน้อยลง 12% สาเหตุเนื่องจากกลุ่มหน่วยงานภาคธุรกิจมีโอกาสจ่ายเงินค่าไถ่มากกว่าผู้ใช้งานทั่วไป

ภาคธุรกิจจึงควรมีข้อมูลแบ็กอัป หรือสำรองไว้ก่อนเกิดเหตุซึ่งจะช่วยลดมูลค่าความเสียหายได้มาก

การแบ็กอัปข้อมูลสามารถทำได้หลายรูปแบบ ไม่ว่าจะเป็นการนำข้อมูลลงในฮาร์ดดิสก์สำรอง การอัปโหลดข้อมูลไปเก็บไว้กับผู้ให้บริการ Cloud ซึ่งแต่ละวิธีการก็มีข้อดีข้อเสียและมีค่าใช้จ่ายแตกต่างกัน

ข้อแนะนำวิธีสำรองข้อมูลเพื่อป้องกันมัลแวร์เรียกค่าไถ่หรือข้อมูลสูญหาย

ควรมีการสำรองข้อมูลอยู่เป็นประจำเพื่อป้องกันข้อมูลสูญหายเนื่องจาก

- ฮาร์ดดิสก์เสียหาย
- เครื่องติดมัลแวร์
- เผลอลบไฟล์โดยไม่ตั้งใจ
- แก้ไขไฟล์ผิดพลาด

คาถาสำรองข้อมูลให้ปลอดภัย (ทำได้เอง)

1. ใช้บริการ **Backup and Restore** ที่มากับระบบปฏิบัติการ
2. สำรองข้อมูลกับ**อุปกรณ์ภายนอก** ไว้มากกว่า 1 ชุด
3. **เข้ารหัสลับ**ข้อมูลที่สำรอง เช่น โปรแกรม Bitlocker ที่มากับระบบปฏิบัติการวินโดวส์
4. สำรองข้อมูลบน **Cloud** ก็เสี่ยงไม่น้อย ฉะนั้นเลือกไฟล์ที่ส่งไปเก็บให้ดี

GO DIGITAL with ETDA

ข้อแนะนำวิธีแบ็กอัปข้อมูลเพื่อป้องกันมัลแวร์เรียกค่าไถ่

การแบ็กอัปลงในฮาร์ดดิสก์แบบเชื่อมต่อภายนอก

- ใช้ File History หรือบริการ Backup and Restore ของ Windows
- หากลักษณะการใช้งานเครื่องคอมพิวเตอร์ เป็นการแก้ไขไฟล์เอกสารอย่างสม่ำเสมอ ควรตั้งค่าความถี่ในการแบ็กอัปข้อมูลให้บ่อยที่สุด เพื่อที่จะสามารถกู้คืนไฟล์ข้อมูลเวอร์ชันล่าสุดได้หากระบบเกิดปัญหา
- หลังการแบ็กอัปเสร็จสิ้น ควรทดสอบให้แน่ใจว่าสามารถกู้กลับคืนได้จริง
- มีความเสี่ยงหากเครื่องติดมัลแวร์ ข้อมูลในฮาร์ดดิสก์สำรองอาจได้รับผลกระทบตามไปด้วย ควรตรวจสอบให้แน่ใจก่อนนำฮาร์ดดิสก์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ หากมีข้อมูลที่สำคัญมาก ๆ อาจพิจารณาแบ็กอัปไว้มากกว่า 1 ชุด

การแบ็กอัปโดยใช้บริการ Cloud

- นำข้อมูลไปฝากไว้กับผู้ให้บริการออนไลน์ที่ให้บริการพื้นที่เก็บข้อมูล
- ข้อดีคือข้อมูลที่อยู่บน cloud สามารถเข้าถึงได้จากอุปกรณ์อื่น ๆ ที่สามารถเชื่อมต่ออินเทอร์เน็ตได้ อีกทั้งในบางบริการสามารถเก็บไฟล์ไว้หลายเวอร์ชัน ทำให้สามารถกู้คืนไฟล์ที่แก้ไขผิดพลาดหรือถูกลบแบบไม่ตั้งใจได้
- ข้อเสียของการสำรองข้อมูลด้วยวิธีนี้คือมีโอกาสที่ข้อมูลอาจรั่วไหลได้

ทั้งนี้ สำหรับผู้ที่สนใจสามารถศึกษาเพิ่มเติมถึงวิธีแบ็กอัปข้อมูลในเครื่องระบบปฏิบัติการ Windows และวิธีแบ็กอัปข้อมูลแบบออนไลน์โดยใช้บริการ Cloud
ได้ที่ http://thcert.co/SK9XIA

อ่านรายละเอียดเพิ่มเติมที่นี่

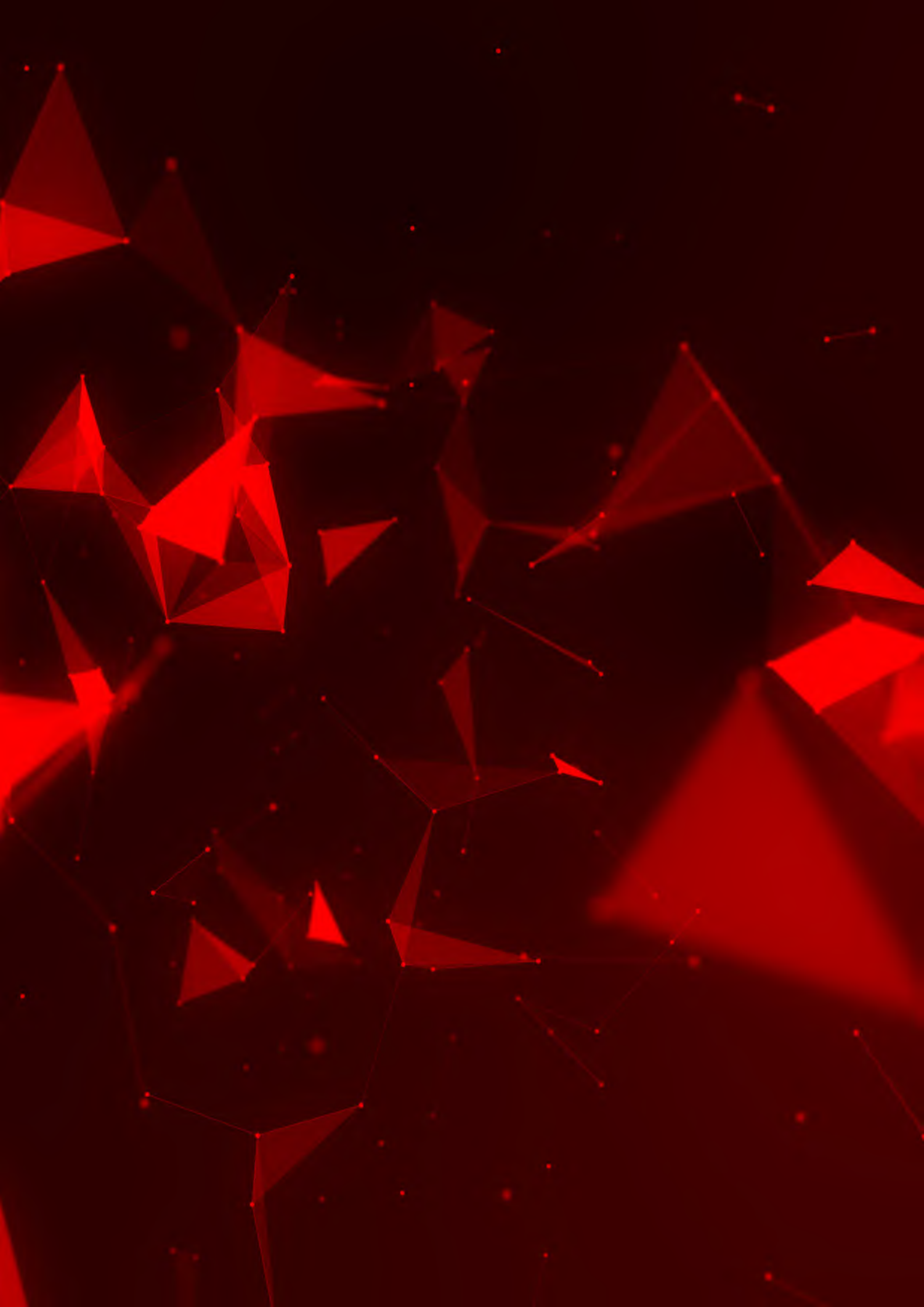
ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ติดตามข่าวสารการแจ้งเตือนและข้อแนะนำด้านความมั่นคงปลอดภัยไซเบอร์
เว็บไซต์ : www.thaicert.or.th
เฟซบุ๊ก : www.facebook.com/thaicert

ปรึกษาเพื่อขอคำแนะนำเพิ่มเติมเพื่อเตรียมพร้อมหรือเมื่อเกิดเหตุภัยคุกคาม
โทรศัพท์ : 0-2123-1212
อีเมล
ติดต่อเรื่องทั่วไป office@thaicert.or.th
แจ้งเหตุภัยคุกคาม report@thaicert.or.th



ThaiCERT a member of ETDA | ETDA สพธอ. www.etda.or.th | กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม

จัดทำโดย
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 15, 20-22 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์ 0 2123 1234 | โทรสาร 0 2123 1200

: ETDA THAILAND

www.etda.or.th