

การรักษาความปลอดภัยทางออนไลน์

เหตุใดความปลอดภัยทางไซเบอร์จึงสำคัญกับฉัน?

อินเทอร์เน็ตและโซเชียลมีเดียเป็นแพลตฟอร์มที่ดีเยี่ยมที่ช่วยให้เราแบ่งปันข้อมูลและติดต่อกับญาติมิตรและครอบครัว

อย่างไรก็ตาม

อาชญากรและองค์กรที่ผิดกฎหมายต่างๆสามารถใช้สื่อออนไลน์เป็นเครื่องมือในการหลอกเอาเงินท่าน ข้อมูลของท่าน หรือข่มขู่ท่าน

อาชญากรดังกล่าวสามารถปฏิบัติการได้จากทั่วทุกมุมโลก
สื่อสารได้อย่างคล่องแคล่วเกือบทุกภาษาและสร้างเว็บไซต์ปลอมได้อย่างแนบเนียน
แก๊งค์ต้มตุ๋นจะติดต่อท่านทางอีเมล โซเชียลมีเดีย และข้อความ
และคนกลุ่มนี้จะพยายามหลอกล่อให้ท่านรู้สึกกลัวหรือวิตกกังวล
เป็นเหตุให้ท่านคิดอ่านได้ไม่รอบคอบ

ทั้งหมดนี้หมายความว่าท่านต้องเตรียมพร้อมและตระหนักถึงกลอุบายที่คนร้ายใช้อยู่เสมอ

ประเด็นทั่วไปที่ฉันอาจพบเจอทางออนไลน์มีอะไรบ้าง?

ต่อไปนี้เป็นสถานการณ์บางส่วนที่เราพบเห็นได้ทั่วไปมากที่สุด

- ท่านได้รับอีเมลหรือข้อความที่น่าสงสัยขอให้ท่านคลิกลิงก์
 - ลิงก์เหล่านี้มักจะนำไปสู่เว็บไซต์ปลอมที่ออกแบบมาเพื่อขโมยข้อมูลการเข้าสู่ระบบหรือรายละเอียดทางการเงินของท่าน
- ท่านได้รับสายโทรศัพท์ที่น่าสงสัยเพื่อขอข้อมูลส่วนตัว
 - ดังที่กล่าวมาข้างต้นผู้โทรจะแสร้งทำเป็นว่ามาจากธนาคารของท่านและขอข้อมูล
- ท่านได้รับการสื่อสารจากบุคคลที่แอบอ้างว่าเป็นผู้มีอำนาจหน้าที่เร่งรีบให้ท่านกระทำการใดๆ
 - หลายนคราที่บุคคลนั้นกระทำการข่มขู่บางอย่าง
- มีผู้เข้าถึงบัญชีออนไลน์ของท่านหนึ่งบัญชีหรือมากกว่านั้น (เช่น อีเมลหรือโซเชียลมีเดีย)

- หากมีผู้เข้าถึงบัญชีออนไลน์ของท่าน คนเหล่านั้นอาจขโมยข้อมูล เปลี่ยนเส้นทางการชำระเงิน และอาจเล็งเป้าหมายไปที่ญาติมิตรหรือครอบครัวของท่านโดยแอบอ้างว่าเป็นท่าน
- รายละเอียดบัตรเครดิตของท่านถูกขโมย หรือท่านถูกหลอกเอาเงินจากการขายหรือการลงทุนปลอม
 - นักต้มตุ๋นหวังว่าท่านจะตกหลุมพรางข้อเสนอที่ล่อใจและประสงค์ที่จะจ่ายเงินโดยไม่คิดลังเล หรือบางกรณีเว็บไซต์จริงอาจโดนละเมิดข้อมูลและรายละเอียดของท่านรั่วไหลทางออนไลน์

มีสถานการณ์เพิ่มเติมดังนี้:

[รับความช่วยเหลือได้ทันที - Own Your Online](#)

ฉันจะออนไลน์อย่างปลอดภัยได้อย่างไร?

- รหัสผ่านที่ยาวและเป็นเอกลักษณ์
 - ยิ่งรหัสผ่านยาวเท่าไรก็ยิ่งเพิ่มความปลอดภัยแน่นหนามากขึ้นเท่านั้น
 - สร้างรหัสผ่านที่จดจำได้มากกว่า 16 อักขระโดยการผนวกคำสุ่มสี่คำเข้าด้วยกัน (เช่น: TriangleRhinoOperationShoes) และเพิ่มตัวเลข ตัวพิมพ์ใหญ่ และสัญลักษณ์หากจำเป็น (เช่น: Triangle&"Rhino"Operation2Shoes)
 - ที่สำคัญคืออย่าใช้รหัสผ่านซ้ำ หากอาชญากรได้รหัสผ่านของท่าน บุคคลนั้นก็จะหาทางเจาะเข้าถึงบัญชีอื่นๆของท่านด้วย
 - [สร้างรหัสผ่านที่ได้ประสิทธิภาพ - Own Your Online](#)
- เปิดใช้งานการตรวจสอบสิทธิ์สองชั้น
 - เหล่านี้เป็นข้อมูลเพิ่มเติม ซึ่งโดยปกติจะเป็นรหัสในโทรศัพท์ของท่านที่ท่านต้องใช้ในการเข้าสู่ระบบเว็บไซต์
 - เทคนิคนี้ปลอดภัยเป็นอย่างยิ่งและสามารถหยุดความพยายามจากคนร้ายส่วนใหญ่ที่จะเข้าถึงบัญชีของท่านได้
 - เราขอแนะนำให้ใช้ "แอปพลิเคชันการตรวจสอบสิทธิ์" หากมีการรองรับฟีเจอร์นี้
 - [ตั้งค่าการตรวจสอบสิทธิ์สองชั้นตอน \(2FA\) - Own Your Online](#)

- ออนไลน์เป็นส่วนตัว
 - ตัวเลือกที่ดีที่สุดในการรักษาความปลอดภัยตามโซเซียลมีเดียคือการเปิดการตั้งค่าความเป็นส่วนตัวของคุณ
 - วิธีนี้จะทำให้คนแปลกหน้ารวมถึงผู้ก่ออาชญากรรมทางไซเบอร์ไม่สามารถดูโพสต์ของคุณหรือส่งข้อความถึงท่านได้
 - [ปกป้องความเป็นส่วนตัวของท่านทางออนไลน์ - Own Your Online](#)
- อัปเดตข้อมูล/อุปกรณ์อิเล็กทรอนิกส์ให้เป็นปัจจุบันอยู่เสมอ
 - เมื่อท่านอัปเดตโทรศัพท์ คอมพิวเตอร์ หรือซอฟต์แวร์ สามารถช่วยปิดช่องโหว่ด้านความเสี่ยงที่อาจเกิดขึ้นได้ด้วยเช่นกัน
 - กลุ่มอาชญากรมักจะมองหาวิธีที่เข้าถึงและอัปเดตแก้ไขช่องโหว่อยู่เสมอ
 - [ท่านต้องหมั่นอัปเดต - Own Your Online](#)
- ต้องระมัดระวังอยู่เสมอ
 - คำแนะนำที่ดีที่สุดคือให้ตระหนักถึงการหลอกลวงเหล่านี้และคอยระวังหากคนร้ายพยายามติดต่อท่านตามแพลตฟอร์มออนไลน์ใดๆ
 - หากเห็นว่าไม่ชอบมาพากลอย่าสนทนากับบุคคลที่ติดต่อท่าน โดยเฉพาะอย่างยิ่งต้องระวังหากมีการเอ่ยขอเงินถึงแม้ว่าคนเหล่านั้นจะดูเป็นมิตรก็ตาม
 - สังเกตลิงก์และที่อยู่อีเมลแปลก ๆ (ตัวอย่างเช่น: ธนาคารของท่านจะไม่ส่งอีเมลจากบัญชี Gmail ถึงท่าน)
 - หากพบข้อสงสัยกรุณาต่อองค์กรโดยตรงและอย่าติดตามลิงก์หรือหมายเลขโทรศัพท์ใดๆที่ท่านได้รับ

ฉันควรทำอะไรหากถูกล่อหรือประสบบกับสถานการณ์ที่ย่ำแย่กว่านั้น?

มีศูนย์บริการหลายแห่งที่ท่านสามารถขอรับความช่วยเหลือได้

องค์กรเหล่านี้จะไม่เปิดเผยรายละเอียดของท่านกับบุคคลอื่น เว้นแต่ท่านจะให้ความยินยอม

- ท่านสามารถรายงานพฤติกรรมทางไซเบอร์ไปยัง NCSC ผ่านทางพอร์ทัล CERT NZ และเราจะให้การช่วยเหลือหรือให้ท่านติดต่อกับหน่วยงานที่เกี่ยวข้องได้:
[รายงานพฤติกรรม | CERT NZ](#)
- หากท่านได้สูญเสียเงินควรติดต่อธนาคารของท่านโดยเร็ว

- สามารถส่งต่อข้อความกลโงงไปยัง 7726
ซึ่งเป็นบริการที่ดำเนินการโดยกรมกิจการภายในโดยไม่เสียค่าใช้จ่าย