

บทความปาถกฐา

เรียบเรียงโดย มายด์มิ่งค์ ผู้ชายสามมิติ

ทำไมพอชคุด... มีจคคณ... บ บ

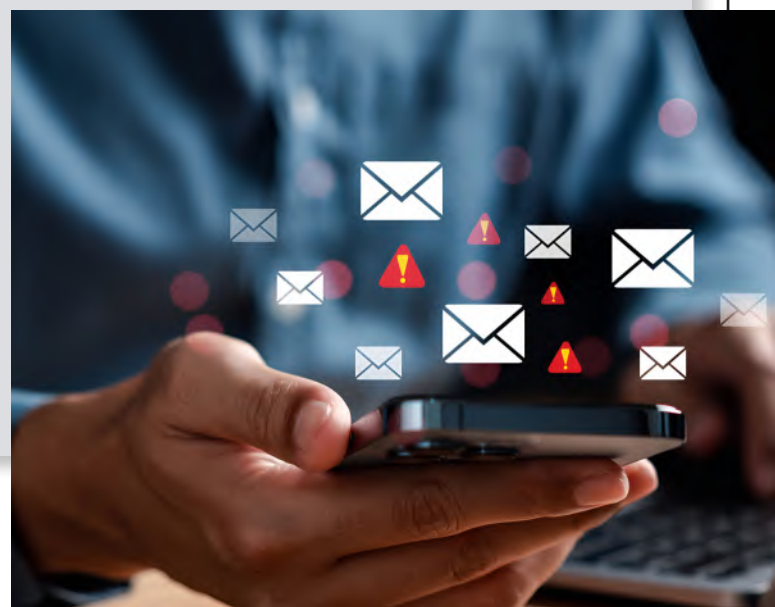


สวัสดีครับ คุณ...(รู้ชื่อเราด้วย)... คุณมีพีสดคุดค้าง
กรุณาติดต่อเจ้าหน้าที่...Blah...Blah...Blah...ได้อัลลอคนี้ น่าจะคุดทุกคน
ถ้าไม่เคยประสบด้วยตัวเอง ก็น่าจะเคยได้ยินจากคนรอบข้าง หรือ
อย่างน้อยที่สุด ผมกล้าพนันเลยว่า คุณผู้อ่านต้องเคยได้แน่ ๆ ว่า
การเริ่มบทสนทนาลักษณะนี้ คงไม่พ้นพวกพีมีจ...(ผาชีพ) แน่ ๆ ถ้า
ย้อนไปเมื่อไม่กี่ปีก่อน เรื่องทำนองนี้ อาจจะเป็นประสบการณ์ตื่นเต้น
แปลกใหม่ ขบขัน และดูเหมือนเรื่องไกลตัว แต่พักหลังมานี้ มีเหยื่อ
จำนวนไม่น้อยที่ถูกหลอก เดิมเป็นตาสีดาสา หรือผู้สูงอายุ โดนหลอก
แต่ปัจจุบันมีคนโดนหลอกทุกระดับ ตั้งแต่เด็ก วัยทำงาน ไปจนถึงระดับ
ดอกเตอร์ ข้าราชการระดับสูง หรือคนที่บางครั้ง เราก็คิดไม่ถึงด้วยซ้ำ
ว่าจะโดนหลอกได้ คิดเป็นความสูญเสียก็ไม่น้อย กลายเป็นปัญหาใหญ่
ของสังคม ไม่ใช่แค่เฉพาะในบ้านเรา แต่เป็นอาชญากรรมระดับโลก!!!

เนื้อหาของเราในวันนี้ เราจะมาทำความรู้จักกับวิธีการ
ต่าง ๆ ที่มีจฉาชีพนิยมใช้ รวมถึงวิธีรับมือ ป้องกันตัวเองไม่ให้ตก
เป็นเหยื่อของกลโกงเหล่านั้นกันครับ การก่ออาชญากรรมแบบนี้
เรียกว่า **อาชญากรรมทางไซเบอร์** ซึ่งมีหลากหลายรูปแบบได้แก่
การโจมตีทางไซเบอร์ อย่างการเจาะระบบคอมพิวเตอร์ การ Hack
ข้อมูล การใช้ Ransom ware เพื่อเรียกค่าไถ่ **การหลอกลวงออนไลน์**
เช่นการหลอกให้โอนเงิน การหลอกขายสินค้าหรือบริการ รวมไปถึง
การเปิดเผยหรือซื้อขายข้อมูลส่วนตัวของเหยื่อ **การเผยแพร่เนื้อหา
ผิดกฎหมาย** เช่นสื่อลามก เนื้อหาหรือข้อความหมิ่นประมาท และ
การละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา เหล่านี้ล้วนก่อให้เกิด
ผลกระทบและความเสียหายทั้งในมิติด้านเศรษฐกิจ การเงิน สังคม
กระทั่งความน่าเชื่อถือและความมั่นคงของรัฐ เป็นปัญหาใหญ่ที่
รัฐบาลของประเทศไหนก็ตามให้ความสนใจและปราบปรามอย่างต่อเนื่อง
มาโดยตลอด แต่น่าเศร้าที่อาชญากรรมและโครงสร้างของปัญหา

ประเภทนี้แก้ไขได้ยาก ด้วยข้อจำกัดด้านทรัพยากรของภาครัฐ
ทั้งในด้านบุคลากร เงินทุน และความก้าวหน้าทางเทคโนโลยี จำนวน
อาชญากรรมเพิ่มขึ้นอย่างรวดเร็ว เพราะสามารถ Work from home
ได้ เพียงแค่มีคอมพิวเตอร์ 1 เครื่องเชื่อมต่อกับอินเทอร์เน็ต :(
ทำให้การป้องกันและปราบปรามมีลักษณะเป็นเชิงรับมากกว่าการ
เชิงรุก เป็นฝ่ายก้าวตามหลังอาชญากรรมอยู่เสมอ

เราจึงไม่สามารถวางใจ ฝากความหวังและบัญชีเงินฝาก
ของเราไว้กับคนอื่น... วันนี้ เราจะมาเรียนรู้เทคนิคคร้อยเล่ห์กลของ
มีจฉาชีพ โดยโฟกัสเรื่องที่ใกล้ตัวพวกเราสักหน่อย อย่างเรื่องการ
หลอกลวงออนไลน์ และการโจมตีทางไซเบอร์ ดีกว่าครับ เริ่มจากเรื่อง
ที่พบบ่อยที่สุด คือการรับโทรศัพท์จากพีมีจฯ หากวิเคราะห์โดย
หลักการแล้ว วิธีที่มีจฉาชีพใช้ได้ผลมากที่สุดคือการอาศัยหลักจิตวิทยา
การโน้มน้าว สร้างสถานการณ์ให้เหยื่อเกิดความตกใจ กลัว วิตกกังวล
ใช้ความโลภของเหยื่อหลอกให้ลงทุน หรือหลอกให้รักแล้วเปย์หนัก ๆ
รัว ๆ โดยมีตัวช่วยในการสร้างความน่าเชื่อถือ เช่นการปลอมแปลง
เอกสารหลักฐานต่าง ๆ การปลอมแปลงตัวตน โดยอาศัยเทคโนโลยี
AI, Deep fake ฯลฯ ให้เหยื่อหลงเชื่อ หลายนกรณีที่เกิดซ้ำบ่อย ๆ
จนกลายเป็นไวรัส และสร้างความเชื่อผิด ๆ ถูก ๆ ขึ้นหลายอย่าง
จริงบ้าง เท็จบ้าง บางเรื่องก็จริงครึ่งเดียว อีกครึ่งหนึ่งถูกบิดเบือน
จากการเล่ากันปากต่อปาก ส่งต่อกันในไลน์กลุ่ม จนปวดหัว คนแก่
ข่าวก็ตามแก๊งจนเหนื่อย คนรับข่าวก็กลัวจนไม่กล้ารับโทรศัพท์
เบอร์แปลก



วิธีการป้องกันตัวจากภัยเหล่านี้คือ

/ อย่าเชื่ออะไรง่าย ๆ ตรวจสอบข้อมูลและแหล่งที่มาของข้อมูลให้ถี่ถ้วนก่อนที่จะเชื่อ

/ อย่ารีบตัดสินใจทันที เพราะหลายกรณีเกิดจากการตัดสินใจผิดอย่างเร่งรีบของตัวเอง

/ อย่าเปิดเผยข้อมูลส่วนตัว และเก็บรักษาข้อมูลอย่างรัดกุม

/ หากเป็นไปได้ กรณีที่เปิดบัญชีออนไลน์ ให้แยกบัญชีเงินเก็บ กับบัญชีที่ใช้สำหรับการใช้จ่าย

ประจำวันแยกจากกัน และทำการตรวจสอบและเปลี่ยนพาสเวิร์ดบ่อย ๆ และเปิดใช้งานระบบยืนยันตัวตน 2 ชั้น (2FA)

/ หมั่นตรวจสอบ e-mail จากธนาคารบ้าง หากมีสิ่งผิดปกติเกิดขึ้น จะได้รับรู้ตัวและหาทางป้องกัน และแก้ไขได้ทันทันที

/ แจ้งเบาะแสหรือข้อมูลเกี่ยวกับอาชญากรรมให้กับหน่วยงานที่เกี่ยวข้อง เช่น กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี หรือสำนักงานตำรวจแห่งชาติ ช่องทางการแจ้งความออนไลน์สามารถแจ้งได้ที่เว็บไซต์ <https://thaipoliceonline.go.th/> และธนาคารที่เรามีบัญชีอยู่



ตำรวจไซเบอร์เตือน 5 อันดับ กลโกง ภัยออนไลน์ใกล้ตัวแห่งปี 2565

- เลือกซื้อจากเว็บไซต์ที่มีชื่อเสียงน่าเชื่อถือ
- ก่อนโอนเงินทุกครั้งให้ระบุตัวตนปลายทางโดยการขอเบอร์โทรศัพท์แล้วโทรไปด้วยเสมอ และบันทึกเสียงไว้เป็นหลักฐาน
- อย่าหลงเชื่อขายคนร้าย ไร้ปลาดึงคอปลาใหญ่
- หลอกให้โอนเงิน โดยได้รับผลตอบแทนจริงในช่วงแรกเท่านั้น
- บัญชีของจริงจะต้องสามารถโทรศัพท์เข้าไปสอบถามได้
- ห้ามลงทุนตามคำชักชวนของผู้ที่รู้จักผ่านทวิตออนไลน์
- คนร้ายมักปลอมใบโปรไฟล์และแอบอ้างโดยใช้รูปภาพของบุคคลที่มีชื่อเสียง
- คนร้ายมักจะหลอกเสียงไม่คุยผ่านวิดีโอคอล

หลอกขายของออนไลน์ **หลอกให้ทำงาน / กู้เงิน** **หลอกให้รักแล้วลงทุน**

หลอกให้กลัวแล้วโอนเงิน เพื่อตรวจสอบความบริสุทธิ์

- ติดตั้งแอปจาก Google Play เท่านั้น
- ห้ามกดลิงก์ที่ส่งมาจากผู้ที่ไม่รู้จักในโลกออนไลน์
- ตรวจสอบชื่อเว็บไซต์ให้ถูกต้องก่อนใส่ชื่อใช้งานและรหัสผ่าน
- หลีกเลี่ยงการเข้าใช้งาน ด้วยการใส่รหัสผ่านแบบ Single Sign On

หมายเลข 1441 www.ThaiPoliceOnline.com

ที่มา: กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี, <https://www.hightechcrime.org/>

การโจมตีทางไซเบอร์ ก็เป็นอีก 1 วิธีที่ได้รับความนิยมในหมู่ที่มิจฉาชีพ เนื่องจากมีต้นทุนต่ำ สามารถเลือกกลุ่มเป้าหมายที่จะโจมตีได้ง่าย ทั้งในแง่ของจำนวนเหยื่อที่ต้องการโจมตี หรือการระบุเหยื่อแบบเฉพาะเจาะจงถือว่าเป็นวิธีการที่มีประสิทธิภาพสูง เหยื่อที่ถูกโจมตีมักจะไม่รู้ตัว และมีมูลค่าความเสียหายค่อนข้างสูงรูปแบบของการโจมตีทางไซเบอร์มีหลายรูปแบบ (อีกแล้ว) ที่คนทั่วไปสามารถพบได้บ่อย ๆ น่าจะเป็นรูปแบบของข้อความที่ส่งมาพร้อมกับลิงค์หน้าตาแปลก ๆ หรืออาจเป็นลิงค์ที่แนบมากับข้อความในรูปแบบของไฟล์ภาพ หรือ QR Code พร้อมกับข้อความชวนเชื่อให้เหยื่อหลงกดเข้าไปหรือเปิดดู... แล้วก็บูมมม...!!! เงินหายเกลี้ยงบัญชีภายในไม่กี่นาที รูปแบบการโจมตีแบบนี้ เรียกว่า ฟิชซิง (Phishing)

สำนักงานตำรวจแห่งชาติ ROYAL THAI POLICE

เคสลงทะเบียนแล้ว สามารถเข้าสู่ระบบได้ทันที เข้าสู่ระบบ

แจ้งความออนไลน์ คดีอาชญากรรมทางเทคโนโลยี

แจ้งความ เฉพาะคดีอาชญากรรมทางเทคโนโลยี

คู่มือการใช้งานระบบแจ้งความออนไลน์

บริการอื่นๆ

- โทร 1441 ศูนย์ AOC บริการ 24 ชั่วโมง
- @police1441 Line Chat แยกบอกให้สำนักงานคดี
- Chat บทกให้คำปรึกษา ความรุนแรงในครอบครัว
- Facebook PCT Police ข้อมูล/ปรึกษา/แนะนำ/แจ้งเบาะแส
- ข้อมูลประสานพันธ์ และเตือนภัย
- ฉลาดโอน Check ready
- ฉลาดโอน ตรวจสอบบัญชีก่อนโอนเงิน

ที่มา: สำนักงานตำรวจแห่งชาติ, <https://thaipoliceonline.go.th/>

ฟิชซิง (Phishing) คือ กลวิธีหลอกลวงทางออนไลน์ มักใช้รูปแบบอีเมลหรือเว็บไซต์ปลอม เลียนแบบองค์กรที่น่าเชื่อถือ เพื่อขโมยข้อมูลส่วนตัว เช่น รหัสผ่าน ข้อมูลบัญชีธนาคาร โดยเหยื่ออาจถูกหลอกให้กรอกข้อมูลหรือคลิกลิงก์ที่ติดตั้งโปรแกรมอันตราย วิธีนี้มักจะใช้กับเหยื่อทุกประเภท ตั้งแต่บุคคลทั่วไป ไปจนถึงองค์กรหรือหน่วยงานใหญ่ ๆ เจื่อนไซที่สำคัญของการโจมตีลักษณะนี้คือเหยื่อจะต้องให้อนุญาต (Grant permission) บางอย่างกับโจร เพื่อการเข้าถึงข้อมูลที่มีฉฉชีพต้องการ ดังนั้น สิ่งที่ต้องระวังให้มากที่สุดคือ **อย่าชี้ชี้้วคลิกคลิค์เด็ดขาด!!!** ไม่ว่าจะเป็นข้อความ sms ไลน์ หรือ e-mail ที่น่าสงสัย

บางครั้ง การโจมตีเหยื่อรายเล็ก ๆ ปลายชีวิต ปลายสร้อย อาจจะไม่น่าใจที่มีจิจา การพลิกแพลง จูโจมด้วยลูกเล่นที่แพรวพราวเหนือชั้นขึ้นมาอีกระดับอย่างการใช้ Malware จึงถูกนำมาใช้กับเหยื่อที่ตัวโตขึ้น การโจมตีลักษณะนี้ ผู้โจมตีจะต้องมีความรู้ทางด้านคอมพิวเตอร์ (Malware) ย่อมาจาก Malicious Software คือ ซอฟต์แวร์ที่ออกแบบมาเพื่อสร้างความเสียหายให้กับระบบคอมพิวเตอร์หรือเครือข่าย มักถูกแฝงมากับโปรแกรมหรือไฟล์ที่ดูน่าเชื่อถือ เพื่อขโมยข้อมูลส่วนตัว ทำลายไฟล์ ติดตั้งโปรแกรมที่ไม่ต้องการ หรือควบคุมระบบคอมพิวเตอร์จากระยะไกล

ดังนั้น ก่อนที่จะกดลิงค์ สแกน QR Code หรือเปิดไฟล์ใด ๆ ก็ตาม จงตั้งสติให้มั่น ตรวจสอบให้แน่ใจว่าข้อมูลมาจากแหล่งที่น่าเชื่อถือ กรณีที่จำเป็นต้องเปิดลิงค์หรือไฟล์ดู ควรนำลิงค์ที่สงสัยไปตรวจสอบว่ามี Malware หรือไม่ จากเว็บไซต์ที่ให้บริการตรวจสอบ Malware ฟรี โดยการใส่ลิงค์ที่ต้องการเปิดดูตรงช่อง URL ได้แก่

- / <https://www.virustotal.com/gui/home/url>
- / <https://www.iswebsitehacked.com/>
- / <https://sitecheck.sucuri.net/https://quttera.com/>

ที่มา: เว็บไซต์กองบังคับการตรวจสอบและวิเคราะห์อาชญากรรมทางเทคโนโลยี, <https://www.hightechcrime.org/cybercrime/malware>



วิธีป้องกันมัลแวร์:

- / ติดตั้งโปรแกรมป้องกันไวรัสและมัลแวร์
- / Update ระบบปฏิบัติการและซอฟต์แวร์ต่างๆ อยู่เสมอ
- / ระมัดระวังดาวน์โหลดโปรแกรมหรือไฟล์จากแหล่งที่ไม่น่าเชื่อถือ
- / ไม่คลิกลิงก์ในอีเมลหรือข้อความที่น่าสงสัย
- / สำรองข้อมูลสำคัญไว้เป็นประจำ

หากสงสัยว่าคอมพิวเตอร์ของคุณถูกมัลแวร์ ให้รีบสแกนหาและกำจัดมัลแวร์ออกจากระบบโดยเร็วที่สุด



สำหรับคนที่ระวังทุกอย่างที่ผมได้กล่าวไปข้างต้นแล้ว ขอแสดงความยินดีด้วยครับ พร็อพสี่นของคุณมีความปลอดภัยขึ้นมาในระดับหนึ่ง แต่ต้องขอยืนยันจริงๆ ที่ต้องบอกว่าคุณยังมีความเสี่ยงอยู่ครับ ถ้าคุณเป็นคนที่ใช้ชีวิตแบบ “ชีวิตติดคอนแทค” เสพติดการใช้มือถือหรือใช้ชีวิตออนไลน์ตลอดเวลา แล้วยังบังเอิญชอบใช้ของฟรีอย่าง Free WiFi ด้วยแล้วละก็... คุณอาจจะตกเป็นเหยื่อของที่มีจซาได้เหมือนกันครับ เนื่องจาก การใช้อินเทอร์เน็ตผ่านสัญญาณ WiFi อาจเสี่ยงต่อการถูกขโมย Username และ Password ของ e-mail, e-Banking ตลอดจนบัญชีผู้ใช้งาน Social Media ต่าง ๆ เนื่องจากข้อมูลที่ส่งผ่านทางสัญญาณไร้สายแบบ WiFi นั้น ไม่มีการเข้ารหัสข้อมูล ดังนั้น เมื่อคนร้ายติดตั้งโปรแกรมสำหรับดักจับข้อมูลบนเครือข่าย WiFi ก็จะสามารถเห็นข้อมูลส่วนตัว ตลอดจนรหัสลับต่าง ๆ ของคุณได้ โดยเฉพาะปัจจุบันนี้ โปรแกรมดักจับข้อมูลสามารถติดตั้งบน Smart Phone ได้เพียงปลายนิ้วสัมผัสเบา ๆ ทำให้ปัญหาหมิ่นแวมโน้มทวีความรุนแรงมากขึ้น โชคดีที่การป้องกันสามารถทำได้ง่าย ๆ โดย

- หลีกเลี่ยงการใช้ WiFi สาธารณะ หรือ Free WiFi ที่คุณอึ้งเอิญไปเจอ ถึงแม้จะมีรหัสผ่านก็มีความเสี่ยง ควรใช้สัญญาณ

จากโทรศัพท์ในการเชื่อมต่ออินเทอร์เน็ต หากจำเป็นต้องใช้ WiFi สาธารณะ ควรรีบเปลี่ยนรหัสผ่านที่เคยใช้ตรวจสอบอีเมล หรือบัญชี Social Media อื่น ๆ เมื่อกลับไปใช้เครือข่ายอินเทอร์เน็ตส่วนตัว

- การใช้อินเทอร์เน็ต ไม่ว่าจะผ่านทาง สาย LAN หรือ WiFi ทั้งที่บ้านและที่ทำงาน ก็ควรเข้ารหัสข้อมูล เพราะคนที่ดักจับข้อมูลสามารถมองเห็นรหัสผ่านและข้อมูลส่วนตัวของท่านได้เช่นเดียวกัน ดังนั้น จึงแนะนำให้ติดตั้ง Extension สำหรับเข้ารหัสข้อมูล ที่ชื่อว่า HTTPS Everywhere ซึ่งรองรับ Browser จากค่าย Firefox, Chrome และ Opera โดยสามารถ Download ได้ที่ <https://www.eff.org/https-everywhere>

อัปเดตอีกนิดก่อนจากครับ... ขณะที่กำลังจะส่งต้นฉบับนี้ บังเอิญเห็นข่าวในมติชนออนไลน์ฉบับวันที่ 11 มีนาคม 2567 เรื่องแก๊งค์อาชญากรไซเบอร์ที่ใช้ชื่อว่า **Gold Factory** เนื้อหาใจความหลักคือมีจซาซีพหลายกลุ่มได้พัฒนาเทคโนโลยีเพื่อโจมตีทางไซเบอร์ บัญชีธนาคารของเหยื่อ และสามารถเจาะผ่านระบบรักษาความปลอดภัยต่าง ๆ ของธนาคาร ได้ด้วยการใช้โทรจัน (Trojan) ในการโจมตีเหยื่อ สามารถเข้าถึงและควบคุมอุปกรณ์มือถือหรือคอมพิวเตอร์ของเหยื่อโดยที่เหยื่อไม่รู้ตัว รายละเอียดในเรื่องข่าวสรุปได้ด้วยคำสั้น ๆ หนึ่งคำว่า “หายน่ะ”

ในฐานะที่เป็นผู้ร่วมชะตากรรมเดียวกับคุณผู้อ่านทุกท่าน ที่ต้องใช้ชีวิตอยู่ท่ามกลางสิ่งวุ่นวายเหล่านี้ ก็ได้แต่กุมขมับและเตือนตัวเองให้ระวังตัว ใช้สติให้มาก และคอยเตือนคนรอบข้างโดยหวังใจว่าทุกท่านจะรักษาตัวให้รอดปลอดภัยจากการโจมตีทางไซเบอร์นะ ครับ... สวัสดีครับ

