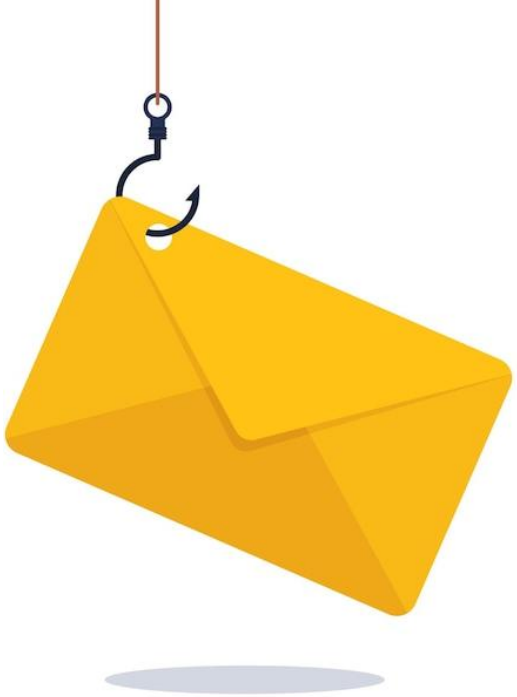


Phishing Email

คืออะไร? ทำไมเราถึงต้องใส่ใจ

Phishing Email คือ ภัยคุกคามทางไซเบอร์ที่ผู้ไม่หวังดีใช้วิธีการหลอกลวงผู้ใช้งานเพื่อขโมยข้อมูลส่วนบุคคล รหัสผ่าน หมายเลขบัตรเครดิต หรือข้อมูลบัญชีธนาคาร โดยมักส่งอีเมลหลอกลวงที่ดูเหมือนมาจากแหล่งที่เชื่อถือได้ ไม่ว่าจะเป็นธนาคาร บริษัท หรือบริการออนไลน์ต่างๆ โดยใน Email Phishing มักจะมีข้อความเร่งด่วนให้เหยื่อตกใจและหลงเชื่อ เช่น การเร่งให้ยืนยันตัวตนภายใน 24 ชั่วโมง หรือบอกว่าบัญชีถูกระงับ พร้อมทั้งมีลิงก์ปลอมที่พาไปยังเว็บไซต์หลอกลวง หรือมีไฟล์ที่ฝังมัลแวร์ไว้ และเมื่อเหยื่อคลิกเข้าไป ก็อาจทำให้ข้อมูลส่วนตัวถูกโจรกรรม หรือระบบของผู้ใช้งานได้รับผลกระทบได้

สิ่งที่สแกรมเมอร์ต้องการ

- รหัสผ่านเข้าระบบ
- เงินทอง
- ข้อมูลส่วนตัว
- ข้อมูลทางการเงิน

วิธีการป้องกันการถูก Phishing

- ตรวจสอบความน่าเชื่อถือของอีเมลผู้ส่ง
- หลีกเลี่ยงการคลิกลิงก์ หรือดาวน์โหลดไฟล์แนบจากอีเมลโดยตรง
- พึงระวังอีเมลที่ขอให้กรอกข้อมูลสำคัญส่วนบุคคล เช่น ชื่อผู้ใช้งาน รหัสผ่าน หมายเลขบัตรเครดิต หรือข้อมูลที่เกี่ยวข้องกับบัญชีออนไลน์
- เปิดใช้งานการยืนยันตัวตนสองขั้นตอน (2FA)
- ติดตั้งโปรแกรม Anti-Virus Anti-Spam และทำการอัปเดตโปรแกรมให้เป็นปัจจุบันอยู่เสมอ
- ตรวจสอบ URL ว่าใช้ https หรือไม่ และมีความน่าเชื่อถือหรือไม่ ส่วนมาก Domain ของเว็บไซต์ที่ส่งมามักจะจดชื่อที่ผู้ใช้มักพิมพ์ผิด หรือชื่อที่ดูเผินๆ แล้ว ใกล้เคียงกับชื่อองค์กรต่างๆ

หากสงสัยว่าตนเองได้รับอีเมลหลอกลวง โปรดติดต่อสอบถามหรือโทรแจ้ง **งานบริการเทคโนโลยี** CITCOMS

หมายเลขโทรศัพท์ **0-5596-1524** เพื่อดำเนินการตรวจสอบ และป้องกันเหตุภัยคุกคาม

Phishing Email
ภัยไซเบอร์ที่ต้องระมัดระวัง

Phishing Email คือ ภัยคุกคามไซเบอร์รูปแบบหนึ่งที่ต้องให้ความระมัดระวังและใส่ใจอย่างมากในปัจจุบัน ซึ่งจะมีรูปแบบในการหลอกลวงโดยการส่งอีเมล โดยจะเริ่มต้นจากข้อความอีเมลที่ดูเหมือนกับว่าเป็นการแจ้งเตือนอย่างเป็นทางการและมีความเร่งด่วนจากแหล่งที่เชื่อถือได้ เช่น หน่วยงานไอทีของมหาวิทยาลัย หน่วยงานราชการ ธนาคาร คนรู้จัก ซึ่งข้อความการแจ้งเตือนดังกล่าวจะทำให้ผู้เสียหายมีความตื่นตระหนกและเกรงกลัว หากผู้เสียหายหลงเชื่อได้กรอกข้อมูลสำคัญต่างๆ ที่แนบมากับลิงค์ในอีเมลหลอกลวงเหล่านี้ เช่น Username และ Password สำหรับการเข้าระบบขององค์กร ข้อมูลส่วนบุคคลอื่นๆ หรือหลอกให้ติดตั้ง Malware จากการคลิกลิงก์หรือไฟล์แนบ ซึ่งจะทำให้ผู้ไม่ประสงค์ดีสามารถโจรกรรมข้อมูลสำคัญเข้าถึงข้อมูลส่วนตัว หรือนำข้อมูลที่ได้ไปปลอมแปลง ส่งผลให้ผู้เสียหายและองค์กรเสื่อมเสียชื่อเสียง หากผู้ไม่ประ สงค์ดีมีการนำข้อมูลที่ได้มาไปใช้งานอย่างผิดกฎหมาย ผู้เสียหายอาจถูกฟ้องร้องดำเนินคดีได้

การโจมตีด้วยฟิชชิ่ง มักจะอยู่ในรูปแบบของข้อความที่ต้องการชักจูงให้คุณทำสิ่งต่อไปนี้

หลอกให้กดลิงก์เพื่อไปเว็บไซต์ปลอม หลอกให้ติดตั้งโปรแกรม หลอกให้ดาวน์โหลดข้อมูล

หลอกเอาข้อมูลที่สำคัญ เช่น ชื่อผู้ใช้งาน รหัสผ่าน เลขบัญชีธนาคาร เลขบัตรประชาชน

หลอกว่าอีเมลเต็ม บัญชีอีเมลมีปัญหา หลอกว่าได้รางวัล หลอกว่าจะให้เงิน

ข่มขู่จะทำให้เสียชื่อเสียง สูญเสียเงิน ข้อมูลสูญหาย เสียเวลาในการแก้ไข

วิธีตรวจสอบ Phishing

ตรวจสอบอีเมลผู้ส่ง

ตรวจสอบชื่อผู้รับ
ว่าสะกดถูกต้องหรือไม่

ตรวจสอบ URL
ของลิงก์ต่างๆ

ตั้งข้อสังเกต
หากมีการร้องขอแปลกๆ

ระวังหากมีการขอ
ข้อมูลส่วนตัวผ่านอีเมล

หากสงสัยว่าตนเองได้รับอีเมลหลอกลวง โปรดติดต่อสอบถามหรือโทรแจ้ง **งานบริการเทคโนโลยี** CITCOMS

หมายเลขโทรศัพท์ **0-5596-1524** เพื่อดำเนินการตรวจสอบ และป้องกันเหตุภัยคุกคาม

สังเกตยังไงให้ปลอดภัย
Phishing Email

มั่นใจว่าไม่เคยมีบัญชีออนไลน์ของเจ้านั้นๆ ที่ส่งอีเมลมา

กรณีนี้ส่วนใหญ่ Phishing email จะแอบอ้างว่าบัญชีของเรามีปัญหา และเกิดข้อผิดพลาดจนไม่สามารถใช้งานกับเว็บไซต์ของที่ทำงาน เช่น “โปรดอัปเดตบัญชี PayPal ของคุณ! ก่อนที่จะไม่สามารถใช้งานได้อีกต่อไป” หากเราไม่มีบัญชีดังกล่าวก็มั่นใจได้เลยว่า นี่คือ Phishing email แน่นอน

ที่อยู่อีเมลสำหรับตอบกลับดูผิดปกติ

ข้อนี้มักจะถูกมองข้ามเสมอ ซึ่งหากตรวจสอบอย่างรอบคอบจะพบว่า สิ่งสำคัญที่จะบอกได้ว่าอีเมลนั้น เป็น Phishing email โดยให้สังเกตจากที่อยู่อีเมลที่ได้รับ @mail.mornor.com ไม่ใช่ @mamar.com

เนื้อความอีเมลมีภาษาผิดหลักไวยากรณ์

เนื้อความใน Phishing email มักจะมีคำที่พิมพ์ผิดออกมาให้เห็น เช่น ใช้ภาษาไม่เป็นทางการ เลือกใช้คำไม่เหมาะสม มีรูปประโยคแปลกๆ จนคาดเดาได้ว่าไม่ใช่อีเมลจากหน่วยงานอย่างแน่นอน

มีข้อความที่เขียนว่า “ด่วนมาก”

เทคนิคที่แฮกเกอร์หลอกลวง คือ การสร้างแรงกดดันให้ต้องจัดการอย่างใดอย่างหนึ่งในทันที เช่น อ้างว่าคุณไม่ได้ชำระเงินตามกำหนด, อ้างว่าคุณเป็นหนี้กับภาครัฐ เป็นต้น

อีเมลที่ได้รับ ไม่ใช่อีเมลที่เคยใช้ติดต่อ

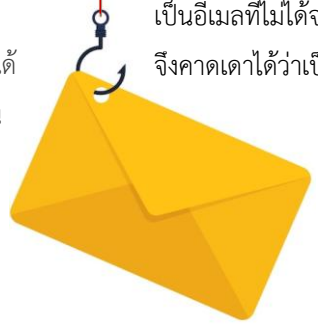
บางครั้งเราอาจจะได้รับอีเมลตอบกลับจากเว็บไซต์ที่เราติดต่อขอให้พิจารณาและตรวจสอบก่อนว่า อีเมลที่รับเชื่อมโยงกันหรือไม่ เราใช้อีเมลอื่นในการติดต่อหรือเปล่า เช่น ได้รับข้อความส่งเข้าอีเมล abc1222@gmail.com แต่ที่จริงใช้อีเมล abc2222@gmail.com

อีเมลที่ส่งมาเพื่อขอให้ยืนยัน Account หรือข้อมูลส่วนตัว

ข้อความใน Phishing email มักจะหนีไม่พ้น เรื่องการให้อัปเดตข้อมูลหรือยืนยันข้อมูลส่วนตัว แม้จะดูน่าเชื่อถือแต่หากทบทวนดีๆ จะพบว่าหลายหน่วยงานประกาศเตือนว่า ไม่มีนโยบายขอข้อมูลส่วนตัวผ่านอีเมลอยู่เสมอโดยเฉพาะธนาคาร ดังนั้น อย่าเผลอคลิกเด็ดขาด

อีเมลที่ไม่ได้ระบุชื่อผู้ใช้งาน ตอนทักทายประโยคแรก

ลักษณะ Phishing email ทั่วไป ที่ไม่ได้เจาะจงโจมตีหน่วยงานใดหน่วยงานหนึ่ง มักจะส่งอีเมลกระจายไปทั่ว โดยรอให้เหยื่อมากดคลิกลิงก์ ซึ่งมักจะใช้คำขึ้นต้นประโยคทักทาย เพื่อทักทายเป็นคำกว้างๆ เช่น Dear valued customer ถ้าเจอคำนี้ แปลว่าเป็นอีเมลที่ไม่ได้จากต้นทางที่รู้จักเรา หรือทำงานร่วมกับเรา จึงคาดเดาได้ว่าเป็น Phishing email



มหาวิทยาลัยนเรศวรมีการจัดอบรมหลักสูตร Cyber Security รวมไปถึงการทำแบบสำรวจ หรือการทดสอบอื่นใด เพื่อวัดความตระหนักรู้ และประเมินความพร้อมในการตอบสนองต่อภัยคุกคามตามมาตรฐานสากลเป็นระยะ