๑. บทความองค์ความรู้

วิธีที่ Office ช่วยปกป้องคุณจากแบบแผนฟิชชิ่ง

บทความนี้จะอธิบายว่าฟิชชิ่งคืออะไร และยังรวมเคล็ดลับวิธีการระบุรูปแบบฟิชชิ่งและทำตามวิธีปฏิบัติเพื่อหลีกเลี่ยงการเป็นเหยื่อของการฉ้อฉลแบบออนไลน์ บทความนี้ยังอธิบายวิธีที่ ระบบ Microsoft Office ๒๐๐๗ ช่วยปกป้องคุณจากรูปแบบฟิชชิ่ง

ในบทความนี้

- ฟิชชิ่งคืออะไร
- ตัวอย่างและลักษณะพิเศษของรูปแบบฟิชชิ่ง
- Office จะช่วยปกป้องฉันจากการหลอกลวงด้วยวิธีฟิชชิ่งและการใช้คำพ้องรูปได้อย่างไร
- วิธีที่ดีที่สุดในการช่วยปกป้องตัวคุณเองจากการฉ้อฉลแบบออนไลน์
- ฉันจะรายงานการฉ้อฉลแบบออนไลน์และการสวมรอยบุคคลได้อย่างไร

ฟิชชิ่งคืออะไร

ฟิชชิ่งคือเทคนิคการฉ้อฉลแบบออนไลน์ที่ใช้โดยอาชญากรเพื่อหลอกล่อให้คุณเปิดเผยข้อมูลส่วนบุคคลของคุณมีเล่ห์เหลี่ยมอยู่หลายแบบที่ใช้เพื่อหลอกล่อคุณ รวมทั้งอีเมลและเว็บไซต์ที่เลียนแบบตราสินค้าที่เป็นที่รู้จักและน่าเชื่อถือ วิธีฟิชชิ่งแบบทั่วไปจะใช้ข้อความปลอมแปลงที่ทำเหมือนว่ามาจากบริษัทหรือเว็บไซต์ที่เป็นที่รู้จัก เช่นธนาคาร บริษัทบัตรเครดิต องค์กรการกุศล หรือเว็บไซต์ซื้อขายของออนไลน์แบบอีคอมเมิร์ซ วัตถุประสงค์ของข้อความปลอมแปลงเหล่านี้คือเพื่อหลอกล่อคุณให้บอกข้อมูลที่ระบุตัวบุคคล (PII) เช่นข้อมูลต่อไปนี้

ชื่อและชื่อผู้ใช้
ที่อยู่และหมายเลขโทรศัพท์
รหัสผ่านหรือ PIN
เลขที่บัญชีธนาคาร
หมายเลขบัตร ATM บัตรเดบิต หรือบัตรเครดิต
รหัสการตรวจสอบบัตร หรือค่าการตรวจสอบความถูกต้องของบัตร (CVV) ของบัตรเครดิต
หมายเลขประกันสังคม (SSN)

ข้อมูลนี้จะถูกใช้ในหลายวิธีเพื่อผลทางการเงิน ตัวอย่างเช่น วิธีทั่วไปคือการสวมรอยบุคคล นั่นก็คือขโมยจะโจรกรรมข้อมูลส่วนบุคคลของคุณ ปลอมตัวเป็นคุณ และสามารถทำสิ่งต่อไปนี้ได้สมัครขอสินเชื่อและได้สินเชื่อในชื่อของคุณถอนเงินในบัญชีธนาคารของคุณจนหมดและใช้จ่ายเต็มวงเงินบัตรเครดิตของคุณ โอนเงินจาก

บัญชีเงินลงทุนหรือวงเงินสินเชื่อของคุณไปยังบัญชีกระแสรายวันของคุณ แล้วใช้สำเนาบัตรเดบิตของคุณเพื่อถอนเงินสดจากบัญชีกระแสรายวันของคุณจากเครื่องรับจ่ายเงินอัตโนมัติ (ATM) ทั่วโลก สำหรับเคล็ดลับเกี่ยวกับวิธีหลีกเลี่ยงไม่ให้ตกเป็นเหยื่อของการฉ้อฉลแบบออนไลน์ ให้ดูที่ส่วนวิธีที่ดีที่สุดในการช่วยปกป้องตัวคุณเองจากการฉ้อฉลแบบออนไลน์ ซึ่งจะอธิบายต่อไปในบทความนี้

ตัวอย่างและลักษณะพิเศษของรูปแบบฟิชชิ่ง

- **ข้อความอีเมลปลอม** ข้อความจะปรากฏเหมือนว่ามาจากบริษัทที่คุณทำธุรกิจด้วย พร้อมกับเตือนคุณว่าบริษัทต้องการตรวจสอบข้อมูลบัญชีของคุณ และถ้าคุณไม่ให้ข้อมูล บัญชีของคุณจะถูกระงับชั่วคราว
- **การรวมไซต์การประมูลสินค้าโดยฉ้อฉลและไซต์ที่หลอกว่าจะให้เงินถ้าทำตามเงื่อนไขที่เสนอ** สิ่งนี้เกิดขึ้นเมื่อมีการนำรายการสินค้าต่างๆ มาตบตาในการประมูลแบบออนไลน์ที่ถูกกฎหมายเพื่อหลอกล่อคุณให้ชำระเงินให้กับไซต์ที่หลอกว่าจะให้เงินถ้าทำตามเงื่อนไขที่เสนอ
- **ธุรกรรมการขายปลอมแบบออนไลน์** อาชญากรจะเสนอซื้อสินค้าบางอย่างจากคุณและขอชำระเงินให้คุณในจำนวนที่มากกว่าราคาของรายการที่อาชญากรนั้นกำลังซื้อ เพื่อเป็นการชดเชย อาชญากรจะขอให้คุณส่งเช็คให้สำหรับส่วนต่างนั้น สุดท้ายจะไม่มีการส่งเงินมาให้คุณ แต่เช็คที่คุณส่งไปถูกนำไปขึ้นเงินและอาชญากรก็เก็บเงินส่วนต่างนั้นไว้ นอกจากนี้ เช็คที่คุณส่งจะมีหมายเลขบัญชีธนาคาร เราท์ติ้งโค้ดของธนาคาร ที่อยู่ และหมายเลขโทรศัพท์ของคุณอยู่ ซึ่งอาชญากรสามารถใช้และได้รับเงินของคุณต่อไปอีก
- **องค์กรการกุศลปลอม** รูปแบบฟิชชิ่งชนิดนี้จะทำเหมือนเป็นองค์กรการกุศลและขอบริจาคเงินโดยตรง โชคไม่ดีที่มีผู้ที่ต้องการเอาเปรียบจากความเป็นคนใจดีของคุณ
- **เว็บไซต์ปลอม** เว็บไซต์นี้จะถูกสร้างให้ดูเหมือนไซต์ที่ถูกต้องตามกฎหมาย เมื่อคุณเยี่ยมชมเว็บไซต์เหล่านี้โดยไม่เจตนา ไซต์จะดาวน์โหลดซอฟต์แวร์ที่มีวัตถุประสงค์ในทางไม่ดีโดยอัตโนมัติ เช่น ไวรัสหรือสปายแวร์ สปายแวร์สามารถบันทึกการกดแป้นพิมพ์ที่คุณใช้เพื่อเข้าสู่บัญชีออนไลน์ส่วนบุคคล ข้อมูลนั้นจะถูกส่งกลับไปยังผู้ทำฟิชชิ่งคุณสามารถป้องกันการหลอกลวงบางชนิดแบบนี้ได้ด้วยการดาวน์โหลดและการติดตั้งซอฟต์แวร์ป้องกันสปายแวร์ เช่นซอฟต์แวร์ป้องกันสปายแวร์ของ Microsoft

ลักษณะโดยทั่วไปของรูปแบบฟิชชิ่ง

เคราะห์ร้ายที่เมื่อการหลอกลวงด้วยวิธีฟิชชิ่งซับซ้อนยิ่งขึ้น จึงเป็นเรื่องยากมากสำหรับบุคคลทั่วไปที่จะบอกว่าข้อความอีเมลหรือเว็บไซต์นั้นมีการฉ้อฉลหรือไม่ นั่นคือเหตุผลที่ว่าเหตุใดรูปแบบฟิชชิ่งจึงแพร่หลายอย่างรวดเร็วและประสบความสำเร็จในหมู่อาชญากร ตัวอย่างเช่น ข้อความอีเมลปลอมและเว็บไซต์ปลอมมากมายจะเชื่อมโยงไปยังโลโก้จริงของบริษัทที่ตราสินค้าที่เป็นที่รู้จัก ดังนั้นอีเมลหรือเว็บไซต์เหล่านี้จึงดูเหมือนถูกกฎหมาย ต่อไปนี้เป็นสิ่งที่คุณสามารถทำเพื่อช่วยปกป้องตัวคุณเองได้

■ **การร้องขอข้อมูลส่วนบุคคลในข้อความอีเมล** ธุรกิจถูกกฎหมายส่วนใหญ่มีนโยบายที่จะไม่ขอข้อมูลส่วนบุคคลของคุณทางอีเมล ดังนั้นให้ตั้งข้อสงสัยกับข้อความที่ขอข้อมูลส่วนบุคคลไว้ก่อนแม้ว่าข้อความนั้นจะดูเหมือนถูกกฎหมายก็ตาม

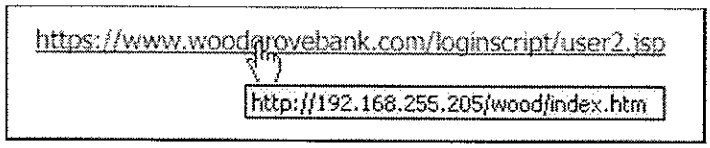
■ **การใช้คำแบบเร่งรัด** การใช้คำในข้อความอีเมลฟิชชิ่งโดยทั่วไปจะสุภาพและมีคำพูดที่ชวนอ่าน ข้อความนี้มักจะพยายามให้คุณตอบกลับข้อความหรือคลิกการเชื่อมโยงที่รวมอยู่ในข้อความ เพื่อเพิ่มจำนวนการตอบสนอง อาชญากรเหล่านี้จะพยายามสร้างความรู้สึกเร่งด่วนเพื่อให้คุณตอบสนองทันทีโดยปราศจากการไตร่ตรอง โดยปกติแล้วจะไม่มีการทำให้ข้อความอีเมลที่ปลอมเป็นแบบส่วนบุคคล ถึงแม้ว่าปกติแล้วข้อความที่ถูกต้องจากธนาคารของคุณหรือบริษัทอีคอมเมิร์ซจะเป็นแบบส่วนบุคคลก็ตาม ต่อไปนี้เป็นตัวอย่างจากรูปแบบฟิชชิ่งที่เกิดขึ้นจริง

"เรียนท่านผู้มีอุปการคุณ ธนาคารมีความประสงค์จะเรียนให้ท่านทราบว่าข้อมูลบัญชีของท่านจำเป็นต้องได้รับการปรับปรุงเนื่องจากการเป็นสมาชิกที่ไม่ได้ใช้งาน การฉ้อฉล และรายงานปลอม ถ้าระเบียนของท่านไม่ได้รับการปรับปรุงจะมีผลให้บัญชีนั้นถูกลบ โปรดคลิกการเชื่อมโยงด้านล่างนี้เพื่อยืนยันข้อมูลของท่าน"

■ **สิ่งที่แนบ** รูปแบบฟิชชิ่งหลายรูปแบบจะขอให้คุณเปิดสิ่งที่แนบ ซึ่งจะทำให้คอมพิวเตอร์ของคุณติดไวรัสหรือสปายแวร์ ถ้าสปายแวร์ถูกดาวน์โหลดลงในคอมพิวเตอร์ของคุณแล้ว จะบันทึกการกดแป้นพิมพ์ที่คุณใช้เข้าสู่บัญชีแบบออนไลน์ส่วนบุคคลของคุณ สิ่งที่แนบใดๆ ที่คุณต้องการเรียกดูควรถูกบันทึกก่อน แล้วสแกนด้วยโปรแกรมป้องกันไวรัสล่าสุด ก่อนที่คุณจะเปิดสิ่งที่แนบนั้น เพื่อช่วยปกป้องเครื่องคอมพิวเตอร์ของคุณ Outlook จะบล็อกชนิดแฟ้มสิ่งที่แนบบางชนิดโดยอัตโนมัติถ้าแฟ้มชนิดนั้นๆ อาจแพร่ไวรัสได้ ถ้า Outlook ตรวจพบข้อความที่น่าสงสัย สิ่งที่แนบของชนิดแฟ้มใดก็ตามในข้อความนั้นจะถูกบล็อก สำหรับข้อมูลเพิ่มเติม ให้ดูวิธีที่ Outlook ช่วยปกป้องคุณจากไวรัส อีเมลที่ไม่พึงประสงค์ และฟิชชิ่ง

■ **การเชื่อมโยงปลอม** ผู้ที่สร้างข้อความฟิชชิ่งมีชั้นเชิงอย่างมากในการสร้างการเชื่อมโยงที่หลอกตาซึ่งทำให้บุคคลทั่วไปไม่สามารถบอกว่าการเชื่อมโยงถูกกฎหมายหรือไม่ วิธีที่ดีที่สุดคือการพิมพ์ที่อยู่เว็บหรือ Uniform Resource Locator (URL) ที่คุณทราบว่าถูกต้องลงในเบราว์เซอร์ของคุณเสมอ คุณยังสามารถบันทึก URL ที่ถูกต้องไปยังรายการโปรดที่เบราว์เซอร์ของคุณได้อีกด้วย อย่าคัดลอกแล้ววาง URL จากข้อความลงในเบราว์เซอร์ของคุณ เทคนิคบางอย่างที่อาชญากรได้ใช้เพื่อปลอมแปลงการเชื่อมโยงเหล่านี้ขึ้นมามีดังนี้

■ **การปิดบังการเชื่อมโยง** แม้ว่าการเชื่อมโยงที่คุณถูกกระตุ้นให้คลิกอาจจะมีชื่อบริษัทจริงทั้งหมดหรือบางส่วน แต่การเชื่อมโยงนั้นอาจจะถูก "ปิดบัง" ซึ่งหมายความว่าการเชื่อมโยงที่คุณเห็นไม่ได้นำคุณไปสู่ที่อยู่นั้นแต่กลับนำไปยังที่อื่นซึ่งมักจะเป็นเว็บไซต์ปลอมแทน ให้สังเกตในตัวอย่างนี้ว่าการวางตัวชี้เหนือการเชื่อมโยงในข้อความ Outlook จะเปิดเผยที่อยู่อินเทอร์เน็ตที่เป็นตัวเลขอื่นในกล่องที่มีพื้นหลังสีเหลือง สิ่งนี้ควรทำให้คุณรู้สึกสงสัย โปรดจำไว้ว่าแม้แต่การเชื่อมโยงในกล่องที่มีพื้นหลังสีเหลืองก็อาจถูกปลอมให้ดูเหมือนที่อยู่เว็บที่น่าเชื่อถือได้



คุณยังควรระวัง URL ที่มีสัญลักษณ์ @ อยู่ด้วย ในตัวอย่าง **https://www.woodgrovebank.com@nl.tv/secure_verification.aspx** URL จะนำคุณไปยังตำแหน่งที่ตั้งที่ต่อจากสัญลักษณ์ @ ไม่ใช่ Wood Grove Bank เนื่องจากเบราว์เซอร์จะละเว้นสิ่งใดก็ตามใน URL ที่อยู่ก่อนสัญลักษณ์ @ ตำแหน่งที่ตั้งจริงซึ่งคือ nl.tv/secure_verification.aspx อาจจะเป็นเว็บไซต์ที่ไม่ปลอดภัยก็ได้

- **คำพ้องรูป** คำพ้องรูป คือคำที่สะกดเหมือนกับคำอื่นแต่มีความหมายแตกต่างกัน ในคอมพิวเตอร์ การหลอกลวงด้วยคำพ้องรูปคือที่อยู่เว็บที่ดูเหมือนกับที่อยู่เว็บที่คุ้นเคยแต่จริงๆ แล้วถูกเปลี่ยนแปลงไป จุดประสงค์ของการเชื่อมโยงเว็บปลอมที่ใช้ในรูปแบบฟิชชิ่งก็คือเพื่อหลอกลวงคุณให้คลิกการเชื่อมโยงนั้น ตัวอย่างเช่น แทนที่จะเป็น **www.microsoft.com** อาจจะปรากฏเป็นดังนี้

  www.micosoft.com

  www.mircosoft.com

ในการหลอกลวงด้วยคำพ้องรูปที่มีชั้นเชิงกว่า ที่อยู่เว็บจะดูเหมือนเว็บไซต์ที่ถูกต้องตามกฎหมายทุกประการ ซึ่งจะเกิดขึ้นเมื่อชื่อโดเมนถูกสร้างโดยใช้อักขระตัวอักษรจากภาษาอื่น ไม่ใช่แค่ภาษาอังกฤษ ตัวอย่างเช่น ที่อยู่เว็บต่อไปนี้ดูเหมือนถูกกฎหมาย แต่สิ่งที่คุณไม่สามารถเห็นได้คือ "i" เป็นอักขระซิริลลิกจากอักษรภาษารัสเซีย

www.microsoft.com

ฟิชเชอร์จะเลียนแบบชื่อโดเมนและชื่อบริษัทอื่นๆ เพื่อหลอกลวงผู้บริโภคให้คิดว่าได้เข้าชมเว็บไซต์ที่คุ้นเคย จำเป็นต้องใช้ซอฟต์แวร์พิเศษเพื่อตรวจหาชื่อโดเมนหลอกลวงชนิดเหล่านี้ในที่อยู่เว็บ โปรดดูหัวข้อถัดไปเพื่อเรียนรู้มากขึ้นเกี่ยวกับวิธีที่ การวางจำหน่าย Office ๒๐๐๗ ช่วยปกป้องคุณจากการเชื่อมโยงที่นำคุณไปสู่เว็บไซต์ที่น่าสงสัย

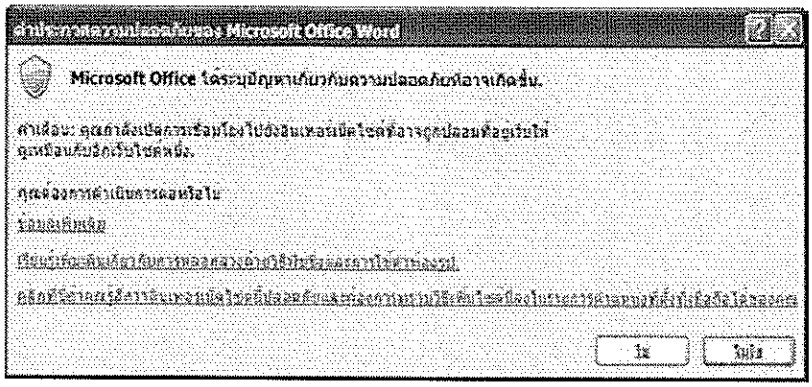
Office จะช่วยปกป้องฉันจากการหลอกลวงด้วยวิธีฟิชชิ่งและการใช้คำพ้องรูปได้อย่างไร

การเชื่อมโยงที่น่าสงสัยในเอกสาร

ตามค่าเริ่มต้น การวางจำหน่าย Office ๒๐๐๗ จะแสดงการแจ้งเตือนความปลอดภัยในสถานการณ์ดังต่อไปนี้

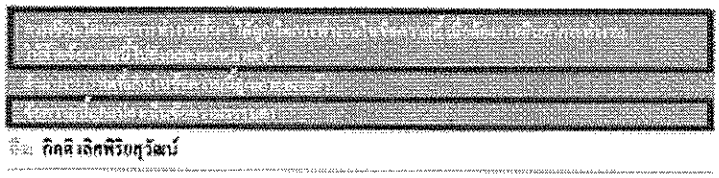
- คุณมีเอกสารที่เปิดอยู่และคลิกการเชื่อมโยงไปยังเว็บไซต์ที่มีที่อยู่ซึ่งอาจเป็นชื่อโดเมนปลอม
- คุณเปิดแฟ้มจากเว็บไซต์ที่มีที่อยู่ซึ่งอาจเป็นชื่อโดเมนปลอม

การแจ้งเตือนเหล่านี้จะปรากฏขึ้นเมื่อคุณคลิกการเชื่อมโยงกับเว็บไซต์ที่มีแนวโน้มว่าใช้ชื่อโดเมนปลอม

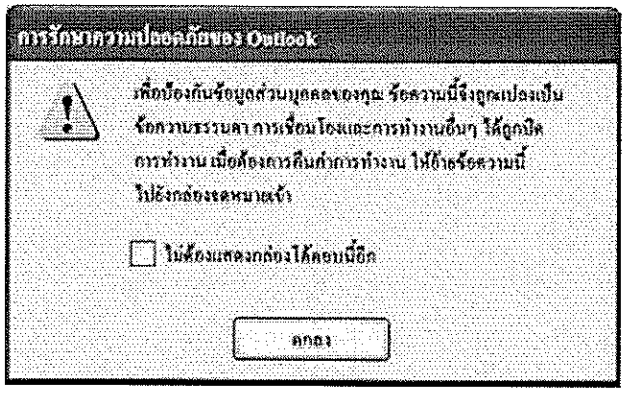


คุณสามารถเลือกได้ว่าจะเยี่ยมชมเว็บไซต์นั้นต่อไปหรือไม่ ในสถานการณ์นี้ เราแนะนำให้คุณคลิก **ไม่** หน้าที่การใช้งานนี้จะช่วยปกป้องการหลอกลวงด้วยคำพ้องรูป สำหรับข้อมูลเพิ่มเติม ให้ดูที่ เปิดใช้งานหรือปิดใช้งานคำเตือนเกี่ยวกับการเชื่อมโยงไปยังเว็บไซต์ที่น่าสงสัยและแฟ้มจากเว็บไซต์ที่น่าสงสัย
การเชื่อมโยงที่น่าสงสัยในข้อความอีเมล ตามค่าเริ่มต้น Microsoft Office Outlook ๒๐๐๗ จะทำสิ่งต่อไปนี้กับข้อความที่น่าสงสัย

- ถ้าตัวกรองอีเมลขยะไม่พิจารณาข้อความว่าเป็นอีเมลที่ไม่พึงประสงค์ แต่พิจารณาว่าเป็นฟิชชิ่ง ข้อความจะถูกทิ้งไว้ในกล่องจดหมายเข้า แต่การเชื่อมโยงใดๆ ในข้อความจะถูกปิดใช้งาน และคุณจะไม่สามารถใช้หน้าที่การใช้งาน 'ตอบกลับ' และ 'ตอบกลับทั้งหมด' ได้
- ถ้าตัวกรองอีเมลขยะพิจารณาข้อความนั้นว่าเป็นทั้งอีเมลที่ไม่พึงประสงค์และข้อความฟิชชิ่ง ข้อความนั้นจะถูกส่งไปยังโฟลเดอร์ **อีเมลขยะ** โดยอัตโนมัติ ข้อความใดที่ส่งไปยังโฟลเดอร์ **อีเมลขยะ** จะถูกแปลงเป็นข้อความธรรมดา และการเชื่อมโยงทั้งหมดจะถูกปิดใช้งาน นอกจากนี้ หน้าที่การใช้งาน 'ตอบกลับ' และ 'ตอบกลับทั้งหมด' จะถูกปิดใช้งานด้วย แถบข้อมูลจะแจ้งเตือนคุณถึงการเปลี่ยนแปลงในหน้าที่การใช้งานนี้



ถ้าคุณคลิกการเชื่อมโยงที่ถูกปิดใช้งานในข้อความฟิชชิ่ง กล่องโต้ตอบ **การรักษาความปลอดภัยของ Outlook** ต่อไปนี้จะปรากฏขึ้น



ถ้าคุณต้องการได้รับแจ้งเตือนถึงความเสี่ยงด้านความปลอดภัยต่อไป ให้คลิก **ตกลง** ถ้าคุณไม่ต้องการได้รับคำเตือนนี้ต่อไปเรื่อยๆ ให้เลือกกล่องกาเครื่องหมาย **ไม่ต้องแสดงกล่องโต้ตอบนี้อีก**

วิธีที่ดีที่สุดในการช่วยปกป้องตัวคุณเองจากการฉ้อฉลแบบออนไลน์

- **อย่าตอบกลับข้อความอีเมลที่ร้องขอข้อมูลส่วนบุคคลของคุณอย่างเด็ดขาด** ให้ตั้งข้อสงสัยกับข้อความอีเมลใดๆ จากธุรกิจหรือบุคคลที่ขอข้อมูลส่วนบุคคลของคุณ หรือผู้ที่ส่งข้อมูลส่วนบุคคลให้คุณและขอให้คุณปรับปรุงหรือยืนยันข้อมูลนั้นให้มาก คุณควรใช้หมายเลขโทรศัพท์จากใบแจ้งยอดของคุณเพื่อโทรศัพท์ติดต่อไปยังธุรกิจนั้นแทน อย่าโทรศัพท์ไปยังหมายเลขที่ปรากฏในข้อความอีเมล ในทำนองเดียวกันอย่าให้ข้อมูลส่วนบุคคลของคุณกับใครก็ตามที่โทรมาหาคุณโดยไม่ได้ร้องขออย่างเด็ดขาด
- **อย่าคลิกการเชื่อมโยงในอีเมลที่น่าสงสัย** อย่าคลิกการเชื่อมโยงในข้อความที่น่าสงสัย การเชื่อมโยงนั้นอาจจะไม่น่าไว้วางใจ แต่ให้เยี่ยมชมเว็บไซต์ด้วยการพิมพ์ URL ของเว็บไซต์ลงในเบราว์เซอร์ของคุณ หรือโดยใช้การเชื่อมโยงในรายการโปรดของคุณแทน อย่าคัดลอกแล้ววางการเชื่อมโยงจากข้อความลงในเบราว์เซอร์ของคุณ
- **อย่าส่งข้อมูลส่วนบุคคลในข้อความอีเมลทั่วไป** ข้อความอีเมลทั่วไปจะไม่ถูกเข้ารหัสลับและจะเหมือนกับการส่งโปสการ์ด ถ้าคุณต้องใช้ข้อความอีเมลเพื่อการทำธุรกรรมส่วนบุคคล ให้ใช้ Outlook เพื่อเซ็นชื่อและเข้ารหัสลับข้อความแบบดิจิทอลโดยใช้การรักษาความปลอดภัย S/MIME ทั้งนี้ MSN, Microsoft Hotmail, Microsoft Outlook Express, Microsoft Office Outlook Web Access, Lotus Notes, Netscape และ Eudora ล้วนสนับสนุนการรักษาความปลอดภัย S/MIME เหมือนกัน
- **ทำธุรกิจกับบริษัทที่คุณรู้จักและไว้วางใจเท่านั้น** ใช้บริษัทที่ก่อตั้งขึ้นและเป็นที่รู้จักอย่างแพร่หลายที่มีชื่อเสียงในด้านการบริการที่มีคุณภาพ เว็บไซต์ทางธุรกิจควรมีคำชี้แจงสิทธิ์ส่วนบุคคลที่ระบุอย่างเฉพาะเจาะจงว่าบริษัทจะไม่ส่งต่อชื่อและข้อมูลของคุณไปยังบุคคลอื่นเสมอ
- **ตรวจสอบให้แน่ใจว่าเว็บไซต์นั้นใช้การเข้ารหัสลับ** ที่อยู่เว็บควรจะนำหน้าด้วย https:// แทนที่จะเป็น http:// ทั่วๆ ไปในแถบ ที่อยู่ ของเบราว์เซอร์ นอกจากนี้ ให้คลิกสองครั้งไอคอนแม่กุญแจ รูปไอคอน บนแถบสถานะของเบราว์เซอร์ของคุณเพื่อแสดงใบรับรองดิจิตอลสำหรับไซต์ ชื่อที่ตามหลัง ออกให้แก่ ในใบรับรองควรตรงกับไซต์ที่คุณคิดว่าคุณเข้าอยู่ ถ้าคุณสงสัยว่าเว็บไซต์นั้นไม่ใช่สิ่งที่ควรเป็น ให้ออกจากไซต์นั้นทันทีและรายงานไซต์ดังกล่าว อย่าทำตามคำแนะนำใดๆ ที่ไซต์นั้นแสดง
- **ช่วยปกป้องพีซีของคุณ** เป็นสิ่งสำคัญที่จะต้องใช้ไฟร์วอลล์ ปรับปรุงข้อมูลในเครื่องคอมพิวเตอร์ของคุณเสมอ และใช้โปรแกรมป้องกันไวรัส โดยเฉพาะอย่างยิ่งถ้าคุณเชื่อมต่อกับอินเทอร์เน็ตผ่านเคเบิลโมเด็มหรือโมเด็ม Digital Subscriber Line (DSL) สำหรับข้อมูลเพิ่มเติมเกี่ยวกับวิธีการทำเช่นนี้ ให้เยี่ยมชมการปกป้องพีซีของคุณ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันไวรัส ให้ดูที่วิธีที่ดีที่สุดในการป้องกันไวรัสและวิธีที่ดีที่สุดในการช่วยป้องป้องกันอีเมลที่ไม่พึงประสงค์ คุณควรพิจารณาการใช้ซอฟต์แวร์ป้องกันสปายแวร์เช่นกันด้วย คุณสามารถดาวน์โหลดซอฟต์แวร์ป้องกันสปายแวร์ของ Microsoft หรือใช้ผลิตภัณฑ์อื่นๆ ที่มีอยู่จากไซต์การดาวน์โหลดและการลองใช้ซอฟต์แวร์รักษาความปลอดภัยได้
- **ตรวจสอบการทำธุรกรรมของคุณ** ตรวจทานการยืนยันใบสั่งของคุณและใบแจ้งยอดบัตรเครดิตและใบแจ้งยอดเงินธนาคารทันทีที่คุณได้รับ เพื่อตรวจสอบให้แน่ใจว่าคุณถูกเรียกเก็บเงินเฉพาะรายการที่คุณใช้ไปเท่านั้น รายงานความผิดปกติในบัญชีของคุณทันทีด้วยการโทรศัพท์ไปยังหมายเลขที่แสดงในใบแจ้ง

ยอดบัญชีของคุณ การใช้บัตรเครดิตเพียงใบเดียวในการสั่งซื้อออนไลน์จะทำให้เป็นเรื่องง่ายขึ้นในการติดตามรายการของคุณ

- **ใช้บัตรเครดิตในการทำธุรกรรมทางอินเทอร์เน็ต** โดยทั่วไป ความรับผิดชอบทางการเงินส่วนบุคคลของคุณในกรณีที่มีใครนำบัตรเครดิตของคุณไปใช้นั้นจำกัดมาก ในทางกลับกัน ถ้าคุณใช้การหักบัญชีอัตโนมัติจากบัญชีธนาคารของคุณหรือจากบัตรเดบิต ความรับผิดชอบทางการเงินส่วนบุคคลของคุณมักจะเท่ากับยอดเงินทั้งหมดของบัญชีธนาคารของคุณ นอกจากนี้ ควรจะใช้บัตรเครดิตที่มีวงเงินต่ำสำหรับการใช้บนอินเทอร์เน็ต เนื่องจากจะจำกัดวงเงินที่สามารถใช้ได้ในกรณีที่บัตรตกไปอยู่ในมือขโมย สิ่งที่ดีกว่านั้นคือผู้ออกบัตรเครดิตหลักหลายรายในปัจจุบันเสนอทางเลือกแก่ลูกค้าในการซื้อสินค้าออนไลน์ด้วยหมายเลขบัตรเครดิตเสมือนสำหรับใช้ครั้งเดียว ซึ่งจะหมดอายุภายในหนึ่งหรือสองเดือน ถ้ามีบริการดังกล่าวในประเทศของคุณ ธนาคารของคุณจะสามารถให้รายละเอียดเกี่ยวกับหมายเลขบัตรเครดิตเสมือนที่มีอายุการใช้งานจำกัดได้

ฉันจะรายงานการฉ้อฉลแบบออนไลน์และการสวมรอยบุคคลได้อย่างไร

ถ้าคุณคิดว่าคุณได้รับข้อความอีเมลที่ฉ้อฉล คุณสามารถรายงานปัญหานั้นและแนบข้อความที่น่าสงสัยได้ การรายงานข้อความที่น่าสงสัยแก่เจ้าหน้าที่จะช่วยในการต่อสู้กับรูปแบบฟิชชิ่ง

๑.ใน Outlook ให้เลือกแต่ไม่ต้องเปิดข้อความที่คุณต้องการรายงาน

๒.บนเมนู การกระทำ ให้คลิก ส่งต่อเป็นสิ่งที่แนบ หรือกด CTRL+ALT+F

๓.ในบรรทัด ถึง ให้พิมพ์ที่อยู่อีเมลของบริษัทที่คุณต้องการรายงานข้อความฟิชชิ่ง ที่อยู่อีเมลบางแห่งซึ่งคุณสามารถใช้เพื่อรายงานเมลที่น่าสงสัยได้คือ

- reportphishing@antiphishing.org จะส่งไปที่ กลุ่มทำงานต่อต้านฟิชชิ่ง ซึ่งเป็นสมาคมอุตสาหกรรมแห่งหนึ่ง
- spam@uce.gov จะส่งไปที่คณะกรรมการการค้าของสหรัฐ (FTC)
- abuse@msn.com จะส่งไปที่ MSN
- abuse@microsoft.com จะส่งไปที่ Microsoft

๔.คลิก ส่ง

ที่มา : *https://support.office.com/th-th*

รวบรวมโดย
กองพัฒนาระบบสื่อสารข้อมูล
ฝ่ายเทคโนโลยีสารสนเทศ

๒. กระทู้

การปฏิบัติตนให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศใน กยท.

ฝทส.ขอเสนอวิธีการปฏิบัติตนให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีสารสนเทศใน กยท. เพื่อให้พนักงานสามารถปฏิบัติงานได้อย่างเต็มประสิทธิภาพ

๑. พนักงานแต่ละท่านควรทำความเข้าใจ และศึกษาเพิ่มเติมเกี่ยวกับระบบงานที่เกี่ยวข้องกับการปฏิบัติงานของตนเอง โดยพนักงานสามารถดาวน์โหลดคู่มือการใช้ระบบงานได้ผ่านทางเว็บไซต์ Intranet ของฝ่ายเทคโนโลยีสารสนเทศ

๒. พนักงานจำเป็นต้องค้นหาข้อมูลเกี่ยวกับผู้ดูแลระบบงานที่เกี่ยวข้อง เช่น หน่วยงานสังกัด หรือหมายเลขโทรศัพท์ติดต่อ เพื่อความสะดวกในการติดต่อประสานงาน

๓. พนักงานต้องหมั่นค้นคว้าหาความรู้ หรือศึกษาเพิ่มเติมเกี่ยวกับเทคโนโลยีในปัจจุบัน เพื่อให้ตนเองสามารถใช้งานเทคโนโลยีได้อย่างคล่องแคล่วมากขึ้น

หากพนักงานท่านใดมีความคิดเห็น หรือความต้องการเพิ่มเติมสามารถเสนอแนะกันเข้ามาได้เลยค่ะ

๓. คำขวัญการจัดการความรู้

“ภารกิจ กยท. ก้าวไกล ด้วยพนักงานใส่ใจพัฒนาองค์ความรู้”