กรุงเทพธุรกิจ
ปีที่ 25 ฉบับที่ 8777 วันพุธที่ 3 ตุลาคม พ.ศ.2555

หน้า 30

เผย 10 เคล็ดลับ เกราะป้องกัน 'อีเมล'

ความสำคัญของ "อีเมล" มีมากขึ้น ทุกวัน เพราะถือเป็นหนึ่งในช่องทางหลักของการสื่อสารยุคนี้ ทั้งยังเป็นเหมือนไอดี (ID) ประจำตัวในการผ่านเข้าไปใช้บริการออนไลน์ต่างๆ ที่มีมากมาย การแฮคอีเมล เพื่อล้วงข้อมูลสำคัญ จนสร้างความเสียหายให้เกิดขึ้นทั้งกับองค์กรธุรกิจ และบุคคลทั่วๆ ไป ก็เลยยังคงมีให้เห็นอยู่อย่างต่อเนื่อง

"กูเกิล" อาสาเผย 10 เคล็ดลับป้องกันอีเมล ดังต่อไปนี้

1.ลงชื่อออกจากระบบระยะไกล การลงชื่อออกจากระบบ (Sign Out) เป็นมาตรการแรกๆ ในการรักษาความปลอดภัยสำหรับอีเมล์ อย่างไรก็ตาม ไม่จำเป็นต้องตกอกตกใจหากคุณลืมลงชื่อออกจากระบบคอมพิวเตอร์ในร้านอินเทอร์เน็ตคาเฟ่ เพราะฟังก์ชันการลงชื่อออกจากระบบระยะไกล (Remote Sign Out) จะช่วยให้คุณสามารถลงชื่อออกจากระบบและปิดเซสชั่นก่อนหน้านี้

2. ใช้การตั้งค่า HTTPS ทุกครั้ง แม้ว่าบัญชีอีเมลของคุณไม่ได้ถูกแฮคอยู่ทุกเมื่อเชื่อวัน แต่ขอแนะนำให้คุณดำเนินทุกมาตรการที่เป็นไปได้เพื่อให้แน่ใจว่าข้อมูลส่วนตัวของคุณจะไม่ตกไปอยู่ในมือของผู้ไม่ประสงค์ดีโดยเฉพาะอย่างยิ่งเมื่อคุณเข้าใช้อีเมลผ่านทางเครือข่ายไร้สายสาธารณะหรือเครือข่ายที่ไม่มีการเข้ารหัส

ตัวอย่างเช่น ตั้งค่า HTTPS แบบอัตโนมัติของจีเมล (Gmail) จะทำให้อีเมลของคุณถูกเข้ารหัสเมื่อมีการรับส่งระหว่างเว็บเบราว์เซอร์ และเซิร์ฟเวอร์ ดังนั้นผู้ใช้ที่ใช้เครือข่ายไวไฟสาธารณะในร้านกาแฟร่วมกับคุณจะไม่สามารถอ่านอีเมลนั้นได้ เว็บไซต์ธนาคารและบัตรเครดิตก็ใช้โปรโตคอลเดียวกันนี้เพื่อปกป้องข้อมูลด้านการเงินของคุณ

หากคุณไปที่ Settings (การตั้งค่า) และเลือก "always use https" (ใช้ https เสมอ) จีเมลก็จะนำคุณไปยังเวอร์ชั่นที่ปลอดภัย

3. ปิดการดาวน์โหลดไฟล์ที่แนบโดยอัตโนมัติ ปิดการใช้งานตัวเลือกสำหรับการดาวน์โหลดไฟล์ที่แนบโดยอัตโนมัติ เมื่อคุณอ่านอีเมล ไฟล์ที่แนบบางไฟล์อาจมีเจตนาที่มุ่งร้าย และตัวเลือกนี้จะช่วยให้

[ต่อด้านหลัง]

การมี 'อีเมลสำรอง' นับว่ามีประโยชน์อย่างยิ่งสำหรับผู้ใช้อีเมลที่มักลืมรหัสผ่านของตัวเองเป็นประจำ

คุณสามารถดาวน์โหลดเฉพาะไฟล์ที่คุณต้องการเท่านั้น และขณะเดียวกันโปรดทราบว่าผู้ให้บริการอีเมลส่วนใหญ่มีฟังก์ชันการสแกนอัตโนมัติ ซึ่งช่วยระบุมัลแวร์หรือไวรัส จึงช่วยปกป้องได้อีกระดับหนึ่ง

4.อย่าไว้ใจใคร หากคุณพบเจอลิงค์ที่ดูเหมือนว่าถูกต้อง แต่คุณก็ยังอดสงสัยไม่ได้ ให้คุณไปที่เว็บไซต์ขององค์กรนั้นๆ โดยตรง เพื่อหลีกเลี่ยงการโจมตีในรูปแบบของฟิชชิ่ง (Phishing) และนอกจากนี้คุณควรตรวจสอบว่ายูอาร์แอล ที่ปรากฏเมื่อคุณวางเมาส์ไว้บนลิงค์กับยูอาร์แอล ที่ระบุไว้ในอีเมลตรงกันหรือไม่

5. กู้คืนรหัสผ่านของคุณผ่านทางข้อความ นอกเหนือจากการร้องขอรหัสผ่านใหม่ทางอีเมลแล้ว คุณยังสามารถลองใช้ตัวเลือกอื่นๆ เช่น การขอรับรหัสผ่านทางระบบรับส่งข้อความ (SMS) บนโทรศัพท์มือถือของคุณ ตัวอย่างเช่น หากคุณมีบัญชี จีเมลคุณก็สามารถปฏิบัติตามขั้นตอนง่ายๆ นั่นคือ คลิกที่ Sign in (ลงชื่อเข้าใช้) จากนั้นเลือก 'Change Password Recovery Options' (เปลี่ยนตัวเลือกการกู้คืนรหัสผ่าน) และป้อนหมายเลขโทรศัพท์มือถือ และบันทึกข้อมูล และเมื่อคุณลืมรหัสผ่าน คุณก็สามารถป้อนชื่อผู้ใช้บนเพจความช่วยเหลือเกี่ยวกับรหัสผ่าน และรหัสกู้คืนก็จะถูกส่งไปยังโทรศัพท์มือถือของคุณ

6. ระวัง "ฟิชชิ่ง" แบบเจาะจงเป้าหมาย ฟิชชิ่งแบบเจาะจงเป้าหมาย (Spear Phishing) อยู่ในรูปแบบของข้อความอีเมลที่เฉพาะเจาะจง ซึ่งอาจดูเหมือนว่าส่งมาจากนายจ้าง หรือเพื่อนร่วมงานที่อาจส่งข้อความอีเมลให้ทุกคนในบริษัท เช่น หัวหน้าฝ่ายทรัพยากรบุคคลหรือฝ่ายไอที โดยปกติแล้ว ผู้หลอกลวงมักจะใช้เว็บแอดเดรส ที่ดูเหมือนชื่อของบริษัทที่มีชื่อเสียง แต่มีการปรับเปลี่ยนเล็กน้อย เช่น เติมหรือลดตัวอักษรบางตัว หรือใช้ตัวอักษรบางตัวที่ดูคล้ายๆ กัน ดังนั้นคุณจึงควรตรวจสอบตัวสะกดให้ดีเสียก่อน

7. อีเมลสำรองก็มีความสำคัญไม่ยิ่งหย่อนไปกว่ากัน การมีอีเมลแอดเดรสสำรองนับว่ามีประโยชน์อย่างยิ่งสำหรับผู้ใช้อีเมลที่มักจะลืมรหัสผ่านของตนเองเป็นประจำ ดังนั้นคุณจึงควรเลือกใช้ผู้ให้บริการอีเมลที่อนุญาตให้คุณระบุอีเมลแอดเดรสสำรองได้ เพื่อรองรับการแจ้งเตือนในกรณีที่คุณไม่มีพื้นที่เก็บข้อมูลเหลืออยู่ หรือแม้กระทั่งในกรณีที่มีกิจกรรมที่น่าสงสัยเกิดขึ้นกับบัญชีอีเมลของคุณ

8. แบ็คอัพข้อมูลอีเมลของคุณในแบบออฟไลน์ ผู้ใช้บางคนอาจต้องการเข้าใช้อีเมลในขณะที่ออฟไลน์ หรือในกรณีที่ไม่สามารถเข้าถึงบัญชีอีเมลของตัวเองได้ ไม่ว่าจะด้วยเหตุผลอะไรก็ตาม ด้วยเหตุนี้คุณจึงควรแบ็คอัพข้อมูลอีเมลของคุณจากบริการออนไลน์

9. ใช้รหัสผ่านที่ไม่ซ้ำกัน นับเป็นความคิดที่ดี ที่คุณจะใช้รหัสผ่านที่ไม่ซ้ำกันสำหรับบัญชีของคุณ โดยเฉพาะอย่างยิ่งสำหรับบัญชีสำคัญๆ เช่น อีเมล และออนไลน์แบงก์กิ้ง เมื่อคุณสร้างรหัสผ่านสำหรับเว็บไซต์ คุณอาจตั้งรหัสผ่าน โดยใช้วลีที่เกี่ยวข้องกับเว็บไซต์นั้นๆ ตัวย่อ หรือคำที่คล้ายคลึงกับวลีดังกล่าว แต่คุณไม่ควรใช้คำที่มีอยู่ในเว็บไซต์ดังกล่าวโดยตรง ตัวอย่างเช่น สำหรับเว็บไซต์ธนาคาร คุณอาจนึกถึงวลีที่ว่า "How much money do I have?" และคุณก็อาจตั้งรหัสผ่านว่า "#m$d1H4ve?" (หมายเหตุ: อย่าเอาตัวอย่างรหัสผ่านที่กล่าวถึงในที่นี้ไปใช้เป็นอันขาด)

10.ใช้ลายเซ็นดิจิทัล ลายเซ็นดิจิทัลเป็นวิธีการตรวจสอบว่าข้อความอีเมลถูกส่งมาจากบุคคลนั้นจริงๆ และไม่ได้ถูกเปลี่ยนแปลงโดยบุคคลอื่น เนื่องจากเป็นการง่ายที่ผู้โจมตีและไวรัสจะ "ปลอมแปลง" อีเมลแอดเดรส ดังนั้นจึงยากที่เราจะระบุข้อความอีเมลที่ถูกต้องในบางครั้ง การรับรองความถูกต้องอาจสำคัญอย่างมากสำหรับจดหมายเพื่อธุรกิจ กล่าวคือ หากคุณไว้ใจให้ใครบางคนตรวจสอบข้อมูล คุณก็จำเป็นที่จะต้องมั่นใจว่า ข้อมูลนั้นมาจากแหล่งที่ถูกต้อง นอกจากนี้ ข้อความที่มีลายเซ็นดิจิทัลยังบ่งชี้ว่าเนื้อหาไม่ได้ถูกเปลี่ยนแปลงหลังที่มีการส่งข้อความดังกล่าว และการเปลี่ยนแปลงใดๆ ย่อมจะทำให้ลายเซ็นดิจิทัลกลายเป็นโมฆะในทันที