อทคอม

ปกป้องข้อมูลสำคัญจากการ Phishing กันเถอะ จบ

วิชญ์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการประจำกระทรวง ICT
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

ต่อจากฉบับที่แล้ว

อย่าหลงเชื่อกลลวงของ Phisher

การจะป้องกันตัวเองให้ปลอดภัยจาก Phisher นั้น โดยปกติแล้วสำหรับผู้ใช้งานทั่วไปก็ควรจะต้องป้องกันคอมพิวเตอร์ของตัวเองเสียก่อน โดยการใช้ Software จำพวก Firewall และ Anti Virus ซึ่งส่วนมากแล้วสามารถป้องกันการ Phishing ได้ดีพอสมควร นอกจากนั้นแล้ว เมื่อจะใช้บริการ Web Site ใดก็ตามที่มีการเชื่อมต่อแบบ SSL (เป็นการเชื่อมต่อโดยใช้ Protocal https คือมีการใช้ใบรับรองอิเล็กทรอนิกส์ หรือ Certificate ส่วนบุคคลในการยืนยันการเชื่อมต่อเข้าสู่ระบบหรือ Web Site) ก็อย่าเพิ่งคิดว่าปลอดภัย ให้ตรวจสอบ Certificate เสียก่อนว่าถูกต้องก่อนจะส่งข้อมูลส่วนตัวออกไปและให้สังเกตส่วนประกอบต่างๆ ใน e-mail ว่ามีส่วนใดน่าสงสัยหรือไม่

ประการแรก หัวจดหมายแบบทั่วไปดูไม่ค่อยน่าเชื่อถือ เช่น Dear Customer ส่วนใหญ่แล้วใครก็เขียนได้ แต่ถ้า e-mail ฉบับนั้นส่งมาจากองค์การจริงก็น่าจะระบุชื่อจริงของเราได้ เพราะองค์การมีข้อมูลส่วนตัวของเราอยู่ แต่ไม่แน่เหมือนกันเพราะ Phisher บางคนก็ปรับเปลี่ยน e-mail ให้ระบุชื่อได้เช่นเดียวกัน

อีกกรณีหนึ่ง คือ การระบุว่า Account ของเรามีปัญหาและต้องการให้แก้ไขอย่างเร่งด่วน เช่น Please reply within 5 days โดยปกติแล้วไม่มีองค์การไหนเร่งรัดลูกค้าจนเกินไปและไม่ยอมเสียลูกค้าง่ายๆ อย่างแน่นอน การเร่งรัดจนเกินไปแสดงว่ามีปัญหาน่าสงสัยและถ้าหากเป็นเช่นนั้นจริง องค์การที่มีประสิทธิภาพจะเลือกติดต่อทางอื่นมากกว่าทาง e-mail

ในการสอบถามข้อมูลส่วนตัวเป็นเรื่องที่ไม่ค่อยกระทำกัน เพราะโดยปกติแล้วธุรกิจต่างๆ จะไม่โทรศัพท์ หรือ e-mail เข้ามาถามข้อมูลส่วนตัวของลูกค้า แต่ในทางกลับกันจะสอบถามก็ต่อเมื่อลูกค้าต้องการข้อมูลส่วนตัวที่อยู่ในระบบเท่านั้นเพื่อเป็นการตรวจสอบตัวลูกค้าเอง ดังนั้น หากมีการติดต่อเข้ามาแล้วถามถึงข้อมูลส่วนตัวให้สงสัยไว้ก่อนว่า เหตุใดองค์การจึงไม่มีข้อมูลของเราอยู่ เช่น ในกรณีขององค์การบัตรเครดิตอาจจะเริ่มต้นสอบถามด้วยหมายเลขโทรศัพท์ หรือที่อยู่ คำถามข้อแรกที่เราควรจะถามกลับก็คือทำไมองค์การถึงไม่มีข้อมูลดังกล่าวและหากองค์การยืนยันว่าไม่มีทำไมจึงสามารถโทรติดต่อโดยตรงได้ รวมทั้งสามารถส่งเอกสารทางจดหมายปกติมาได้อย่างถูกต้องและหากเป็น e-mail Phishing ถ้า Link มีความยาวมากกว่าปกติ ให้สงสัยไว้ก่อนว่า Link ดังกล่าวไม่น่าไว้ใจและหากมีเครื่องหมาย @ หรือมีการสะกดผิด เราสามารถ

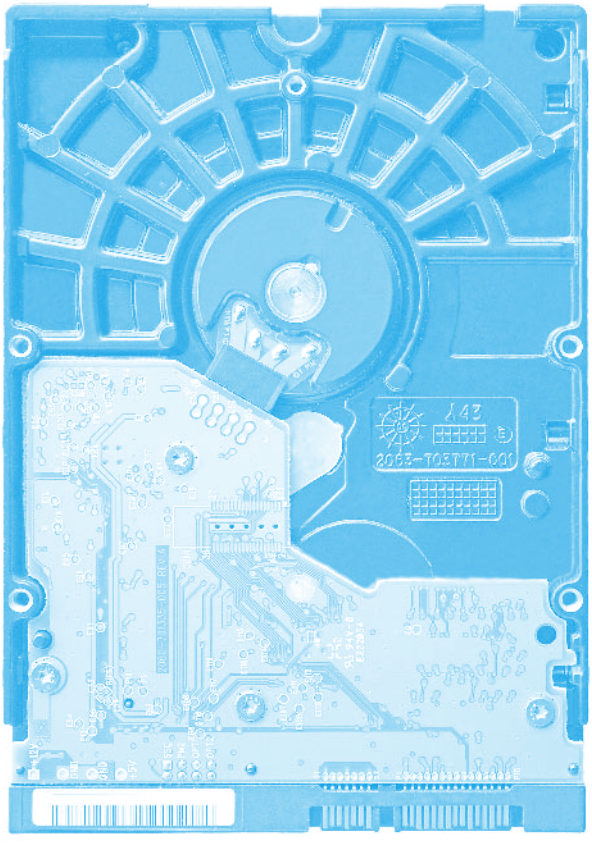
ระบุได้ว่านี่คือ e-mail Phishing และถ้าไม่แน่ใจจริงๆ ก็ให้เปิด Web Browser แล้วพิมพ์ URL ลงไปด้วยตัวเองแทนการคลิกที่ Link

ป้องกันตัวไม่ให้เป็นเหยื่อ

ดังที่กล่าวไปแล้วว่า ไม่มีทางที่เราจะปลอดภัยได้ร้อยเปอร์เซ็นต์ ดังนั้นหากต้องการให้มั่นใจที่สุดแล้ว สิ่งแรกที่ต้องคิดเอาไว้เสมอก็คือ อย่าหลงเชื่อ e-mail ใดๆ และเชื่อไว้เสมอว่าทุก e-mail ที่ส่งมานั้นน่าสงสัยเอาไว้ก่อน เพราะทั้งข้อความและส่วนหัวของ e-mail จนกระทั่งรวมไปถึงชื่อผู้ส่งสามารถปลอมแปลงได้ เราจึงไม่ควรไว้ใจอีกต่อไปและแม้แต่ e-mail Server ก็อาจจะเป็นของปลอมได้ ต่อมาให้ตรวจสอบข้อมูลใน e-mail เสียก่อน โดยปกติแล้วภาษาที่ใช้จะต้องดีพอ หากมีการใช้ภาษาไม่ถูกต้อง ให้เชื่อไว้ได้เลยว่าเป็น Phishing โดยเฉพาะหากมีการสะกดผิด เช่น citibnk เพราะองค์การใหญ่ๆ คงไม่ยอมให้เกิดเรื่องผิดพลาดแบบนี้แน่นอนและเมื่อได้รับ e-mail แล้วไม่ควรคลิก Link ใดๆ รวมทั้งไม่ควรเปิดแนบ File ที่ส่งมาด้วยกัน เพราะนั่นจะนำเราไปสู่การเป็นเหยื่อทั้งสิ้น

นอกจากนี้ยังไม่ควรจะส่งข้อมูลส่วนตัว ใดๆ ก็ตามของเราผ่านไปทาง e-mail เพราะบนเส้นทางกว่าจะถึงปลายทางนั้นอาจจะถูกดักจับได้ทุกเมื่อ แต่ถ้าเลี่ยงไม่ได้จริงๆ ก็ควรจะเข้ารหัสเอาไว้ก่อน นอกจากนั้นแล้วในกรณีที่ใช้บริการ On-line ต่างๆ ที่เกี่ยวข้องกับค่าใช้จ่าย หรือการเงินทั้งหมด ไม่ควรใช้ Password เดียวกัน ควรจะเปลี่ยน Password ไปเรื่อยๆ ไม่ให้ซ้ำกัน เพื่อป้องกันการโดนโจมตีพร้อมกันจากหลายๆ แหล่งและหมั่นตรวจสอบบริการ On-line อยู่เสมอและเช็ครายการต่างๆ ว่าถูกต้องหรือไม่อีกด้วย

สุดท้ายถ้าหากจำเป็นต้องติดต่อไปยังบริการขององค์การผ่านทาง Internet แม้จะมีการเชื่อมต่อแบบ SSL ก็ไม่ควรไว้ใจ ให้คลิกตรวจสอบ Certificate ก่อนเสมอ หรือเลือกที่จะเป็นผู้ติดต่อเข้าไปหา ไม่ใช่ให้องค์การติดต่อเข้ามา



และถ้าหากทุกข้อที่กล่าวมานั้นยังไม่สามารถป้องกันได้และหลงเป็นเหยื่อไปเสียแล้ว สิ่งที่จำเป็นต้องทำก็คือ ติดต่อองค์การผู้ให้บริการบัตรเครดิตก่อนเป็นอันดับแรก โดยระบุว่าบัตรอาจจะถูกขโมยข้อมูล แล้วให้ขอคำปรึกษาจากพนักงานเสียก่อน ถึงตรงนี้ถ้าพนักงานแนะนำให้หยุดการใช้บัตรเอาไว้ชั่วคราวหรือยกเลิกบัตรดังกล่าวก็ควรจะต้องทำและถ้าหากมีบัตรมากกว่าหนึ่งชุด ให้ตรวจสอบบัตรทุกใบเช่นกัน จากนั้นอาจจะต้องติดต่อไปยังธนาคารเจ้าของบัตรเพื่อป้องกันปัญหา หรือหาวิธีแก้ไข แล้วเปลี่ยน Password บริการ On-line ทันที นอกจากนี้แล้วยังอาจจะต้องเข้าไปเปลี่ยน Password ใน Web Site อื่นๆ ที่น่าจะเกี่ยวข้องตามไปด้วยเช่นกันเพื่อป้องกันไม่ให้ Phisher เอาข้อมูลที่ได้ไปทดลองใช้กับ Web Site หรือบริการแห่งอื่นๆ

ทางออกสำหรับองค์การ

สิ่งที่องค์การต้องทำและเตรียมรับมือกับ Phishing โดยเฉพาะกับองค์การคู่ค้า หรือสถาบันการเงินต่างๆ ก็คือ จะต้องทราบการโจมตีของ Phisher ให้ได้เร็วที่สุดและเข้าไปแก้ไข หรือแจ้งเตือนลูกค้าให้เร็วที่สุด เพื่อจะลดมูลค่าความเสียหายที่เกิดขึ้นให้ต่ำที่สุดเช่นกัน โดยถ้าหากมีการตรวจสอบพบก็ควรจะต้องแจ้งเตือนบน Web Site ทันทีและควรจะต้องมอนิเตอร์ DNS อยู่เป็นประจำและตรวจสอบการสื่อสารเข้าไปยัง Web Site หากมีการแก้ไขที่ DNS เมื่อไหร่ก็จะต้องรีบกู้คืนให้เร็วที่สุด หรือหากช่วงใดมีการเข้ามาใช้บริการที่ Web Site น้อย หรือมากผิดปกติให้ตั้งข้อสังเกตไว้ก่อน ว่าอาจจะมีการโจมตีเกิดขึ้นแล้วที่ในหรือนอกองค์การ เพราะถ้าหากมีการเข้ามาใช้บริการเกินไปก็อาจจะเป็นไปได้ว่ามี Web Site ปลอมเกิดขึ้น แล้วลูกค้าหลงเชื่อไปเข้า Web Site ปลอมเสียแล้วส่วนหนึ่ง ซึ่งอาจจะใช้บริการขององค์การที่มอนิเตอร์ให้เราก็ได้เช่นกันแทนที่จะต้องเสียเวลาให้พนักงานตรวจสอบ

นอกจากนี้แล้ว Software Anti Spam มักจะมีความสามารถในการตรวจจับ Phis-

hing ได้เช่นกัน ซึ่งหากมีการ Update อย่างสม่ำเสมอก็จะสามารถช่วยป้องกันได้ในระดับหนึ่ง แต่ถึงอย่างไรนอกเหนือจากการป้องกันขั้นพื้นฐานแล้ว ก็ยังอาจจะต้องปรับเปลี่ยนพฤติกรรมการทำงานเสียใหม่เช่นกัน

การป้องกันโดยการใช้ระบบการเข้าถึงระบบ (Access Control) ที่แน่นหนามากขึ้น วิธีนี้จำเป็นให้ทุกๆ ผู้ใช้ที่ต้องการเข้าสู่ระบบเปลี่ยนแปลงพฤติกรรมการใช้งานของตัวเองเสียใหม่ โดยจะต้องมีการ authentication ในรูปแบบที่ปลอดภัยมากขึ้น เช่น การใช้อุปกรณ์ทางกายภาพเป็นอุปกรณ์ในการ authentication เช่น Smartcard หรือ RFID เป็นต้น ข้อดีของการแก้ปัญหาด้วยวิธีนี้ก็คือการเข้าสู่ระบบมีการตรวจสอบที่แน่นหนามากขึ้น ถึงแม้ผู้ใช้จะตกเป็นเหยื่อของ Phisher แต่ท้ายที่สุด Phisher ก็ไม่สามารถเข้าสู่ระบบได้ หากว่าไม่มีอุปกรณ์ที่จำเป็นดังกล่าวและผู้ใช้เองก็จะได้ความรู้สึกมั่นใจมากขึ้นในการใช้ Web Site ธุรกิจ แต่วิธีนี้ก็มีข้อเสียก็คือผู้ใช้จะต้องใช้เวลาศึกษาให้เข้าใจและขั้นตอนการติดตั้งระบบก็ยังต้องใช้เวลา รวมทั้งมีการติดตั้งซอฟต์แวร์ที่เดสก์ทอปและยังมีค่าใช้จ่ายในการดูแลรักษาค่อนข้างสูง โดยภาพรวมแล้ววิธีนี้จะเหมาะสำหรับองค์การที่มีพนักงานจำนวนไม่มากนักและต้องการความปลอดภัยสูงจริงๆ

ทางออกที่สองคือการใช้ Authentication สำหรับ e-mail Server ซึ่งทางออกนี้ Anti-Spam Research Group พบว่าปัญหาเริ่มมากขึ้นเรื่อยๆ จึงหาวิธีป้องกันโดยไอเดียง่ายๆ ก็คือการเข้าไประบุที่ Server ว่ามีใครบ้างที่สามารถส่ง e-mail โดยใช้ IP Address หรือ e-mail Server ตามที่ระบุได้บ้าง ซึ่งวิธีนี้จะ Config ระบบได้ค่อนข้างง่ายมากและ Phisher ก็จะกลายเป็นบุคคลที่มีตัวตนและสามารถตรวจสอบได้ รวมทั้งยังลดโอกาสเกิด Spam ได้มากเช่นกัน แต่ในทางกลับกันทั้ง Server ของผู้ส่งและผู้รับต้องสนับสนุนวิธีเดียวกัน แต่ถึงอย่างไรในช่อง From: ก็ยังสามารถแก้ไขได้อย่างอิสระเช่นกันและยังส่งผลให้ไม่สามารถใช้บริการ e-mail forwarding ได้อีกด้วย

ทางออกที่สามคือการใช้ลายเซ็นดิจิตอล (Digital Signature) สำหรับ e-mail และตรวจสอบความถูกต้องที่เครื่อง Client โดยเทคนิคนี้จะใช้ S/MIME ซึ่งเป็นมาตรฐานที่มีใช้กันอยู่ทั่วไปมาช่วย โดยหากองค์การที่มีความเสี่ยงในการโดนโจมตีด้วย Phishing ก็อาจจะหันมาส่ง e-mail ไปพร้อมกับลายเซ็นดิจิตอล โดยลายเซ็นดิจิตอลอาจจะถูกแนบไปที่ Gateway เพื่อให้ง่ายต่อการใช้งานของผู้ใช้ ทำให้ผู้ใช้ไม่ต้องเสียเวลากับลายเซ็นดิจิตอลเมื่อรับ e-mail โดย e-mail Client ต่างๆ ก็จะพบว่า e-mail มีลายเซ็นดิจิตอลแนบมาด้วย แต่ถ้าหากรับแล้วไม่มีลายเซ็นดิจิตอลก็มั่นใจได้เลยว่าเมลนี้เป็นของปลอม ข้อดีของวิธีนี้คือง่ายและสะดวกมากอีกทั้งยังไม่สามารถปลอมชื่อในช่อง From: ได้ และหาก Phisher ต้องการส่ง e-mail ที่มีลายเซ็นดิจิตอลจริงๆ ก็จะต้องไปลงทะเบียนกับ Certificate Authority (CA) ซึ่งก็จะเป็นการเปิดเผยตัวตนของเขาเองและนอกจากนั้นแล้วผู้ใช้ หรือลูกค้าขององค์การยังสามารถตรวจสอบความถูกต้องได้อีกด้วย แต่ปัญหาของวิธีนี้ก็คือผู้ใช้ส่วนใหญ่ไม่ค่อยสนใจเรื่องของลายเซ็นดิจิตอลและไม่เคยรู้จัก หรือสังเกตเสียด้วยซ้ำ นอกจากนี้แล้ว Phisher ยังอาจจะปลอมตัวโดยใช้ชื่อในช่อง From: ให้สะกดคล้ายๆ กับ e-mail ของจริงแล้วไปลงทะเบียนเอาไว้ก็จะได้ลายเซ็นดิจิตอลของจริง ซึ่งหากไม่สังเกตให้ดีก็จะเข้าใจว่านี่คือ e-mail จริงเพราะมีลายเซ็นดิจิตอลถูกต้องเสียด้วย

วิธีที่สี่คือการใช้ลายเซ็นดิจิตอลและตรวจสอบที่ Gateway โดยวิธีนี้จะลดภาระของผู้ใช้และผู้ใช้จะมองไม่เห็นการใช้ลายเซ็นดิจิตอลอีกต่อไป โดยที่ e-mail ที่ส่งออกมาจะถูกใส่ลายเซ็นดิจิตอลที่ Gateway จากนั้นเมื่อส่งมาถึง Gateway ปลายทางก็จะมีการตรวจสอบลายเซ็นดิจิตอลเสียก่อนว่าเป็นของจริงพร้อมทั้งตรวจสอบ Domain ไปพร้อมๆ กัน ซึ่งถ้าหากมีข้อผิดพลาดที่จุดดังกล่าว e-mail นั้นจะถูกมองเป็น Phishing ทันที วิธีนี้ค่อนข้างได้รับความนิยมและใช้งานค่อนข้างสะดวกสำหรับ ISP และผู้ให้บริการ Website หรือ e-mail ต่างๆ

บทสรุป ไม่ว่าจะมีวิธีป้องกันอย่างไรทั้งในส่วนขององค์การและผู้ใช้ภายในองค์การเองก็ตาม สุดท้ายแล้ว Phisher ก็จะหาวิธีโจมตีเข้ามาจนได้ ซึ่งก็ขึ้นอยู่กับผู้ใช้ที่จะต้องป้องกันและระวังตนเองและไม่อยู่ในกลุ่มเสี่ยงที่จะตกเป็นเหยื่อของ Phisher ไม่ให้ข้อมูลส่วนตัวกับใครก็ตามที่เราไม่ไว้ใจ รวมทั้งสินค้าและบริการหลายๆ อย่างบน Internet ที่น่าสงสัย เช่น สินค้าที่มีราคาถูกผิดปกติ หรือสินค้าที่ดูแปลกเกินไป รวมทั้งพฤติกรรมการสอบถามข้อมูลของ Web Site เองที่ไม่น่าไว้ใจ ล้วนแต่เป็นช่องทางเสี่ยงด้วยกันทั้งสิ้น ถึงเวลาแล้วที่เราควรจะเตรียมตัวให้พร้อมในยุคที่เทคโนโลยีเข้ามามีบทบาทต่อชีวิตมากขึ้นในทุกๆ ด้าน ซึ่งมีผู้ไม่หวังดีอาศัยประโยชน์กระทำการที่ไม่พึงประสงค์จนถึงขั้นเป็นการก่ออาชญากรรมบนโลกไซเบอร์ เราจึงควรที่จะต้องกลับมายืนในตำแหน่งที่ปลอดภัยจากการถูกล่อลวงและระวังตัวอยู่อย่างสม่ำเสมอเพื่อรักษาผลประโยชน์ของตัวเองและองค์การของเรา TPA