วิชญ์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการประจำกระทรวง ICT
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

ปกป้องข้อมูลสำคัญจากการ Phishing กันเถอะ

หนึ่งในเทคนิคการโจมตีผ่านทาง Internet หรือแม้แต่บริการ On-line รูปแบบอื่นที่นับวันจะเพิ่มขึ้นเรื่อยๆ ก็คือการโจมตีในรูปแบบที่เรียกว่า **Phishing** ซึ่งไม่เพียงแต่สร้างความรำคาญให้กับผู้รับ e-mail ที่มีการโจมตีในรูปแบบนี้ เพียงอย่างเดียวเท่านั้น แต่ Phishing ยังก่อให้เกิดความเสียหายเป็นอย่างมาก ทั้งทางตรงและทางอ้อม ซึ่งหากประเมินเป็นค่าใช้จ่ายแล้วอาจจะเรียกได้ว่าสูงมากเลยทีเดียว

Phishing *คือ การโจมตีในรูปแบบของการปลอมแปลง e-mail (e-mail Spoofing) และทำการสร้าง Web Site ปลอม เพื่อทำการหลอกลวงให้เหยื่อ หรือผู้รับ e-mail เปิดเผยข้อมูลทางด้านการเงิน หรือข้อมูลส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลขบัตรเครดิต บัญชีผู้ใช้ (Username) และรหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่นๆ โดยจะเรียกบุคคล หรือกลุ่มคนที่ทำการเหล่านี้ว่า* ***Phisher***

ปัจจุบันมีภาพยนตร์หลายเรื่องที่กล่าวถึงการขโมยข้อมูลส่วนตัว หรือแม้แต่การขโมย Identity ออกมาให้รับชมกันอยู่เป็นระยะ แต่ท้ายที่สุดแล้วนั่นก็เป็นเพียงเรื่องราวในภาพยนตร์ที่ผู้ชมได้ความรู้สึกหรืออารมณ์ร่วมตั้งแต่เริ่มต้นจนจบและทุกอย่างก็ดูเหมือนจะจบลงหลังจากระยะเวลาประมาณ 2 ชั่วโมงในโรงภาพยนตร์ผ่านพ้นไป แต่ไม่มีใครเคยคิดว่าถ้าสิ่งที่เกิดนั้น คือ เรื่องจริงที่อาจต้องเจอกันอยู่วันละ 24 ชั่วโมงและไม่มีจุดสิ้นสุด

หากวันหนึ่งข้อมูลส่วนตัวของเราถูกขโมยไปใช้งานในทางที่ผิด ซึ่งเมื่อเราสูญเสียความเป็นตัวเองไปให้กับใครสักคนหนึ่งที่สามารถปลอมตัว เป็นตัวเราได้อย่างแนบเนียน ผลเสียที่เกิดขึ้นไม่ได้มีเพียงแค่เจ้าของข้อมูลที่ถูกขโมยไปเท่านั้น แต่ยังมีอีกหลายคนที่เสียผลประโยชน์ตามไปด้วยเช่นกัน แน่นอนว่าเราเองก็คงเป็นผู้เสียผลประโยชน์คนแรกและต่อมาก็คือองค์การที่เราเกี่ยวข้องทั้งหมด ระบบความปลอดภัยภายในองค์การที่ขาดความน่าเชื่อถือและไว้ใจไม่ได้อีกต่อไป หากเป็นองค์การใหญ่ความเชื่อมั่นที่หายไปย่อมหมายถึงผลกำไรที่สูญหายไปด้วยเช่นกัน นอกจากนั้นก็ยังรวมไปถึงองค์การที่เราเองไปเป็นลูกค้าและโดนโจมตี

นอกจากจะเสียความเชื่อมั่นแล้วก็ยังสูญเสียรายได้จากการนำข้อมูลที่ขโมยมาแล้วนำมาใช้งาน สมมุติง่ายๆ ว่าธนาคาร A ถูกเลือกเป็นเหยื่อล่อ แล้วเราเองก็หลงเชื่อ Phisher ส่งข้อมูลส่วนตัวพร้อมหมายเลขบัตรเครดิตกลับไปให้ Phisher แน่นอนว่าสิ่งแรกที่เกิดตามมาก็คือบัตรถูกขโมยไปใช้ เราเองต้องสูญเงินก้อนโตผ่านทางบัตรเครดิต ซึ่งกว่าจะรู้อย่างน้อยที่สุดก็สิ้นเดือน หรือถ้าไม่เคยสังเกตรายการใน Slip บัตรเครดิตก็อาจจะกินเวลาหลายเดือน ซึ่งถ้าหากเรารู้ตัวและเอะใจขึ้นมา แน่นอนว่า

ความเชื่อมั่นต่อระบบความปลอดภัยในองค์การก็จะสูญเสียไปในทันทีและผลที่ตามมาคือธนาคารอาจจะต้องเป็นผู้รับผิดชอบต่อความเสียหายเป็นรายต่อไป แถมยังจะเสียลูกค้าเนื่องจากเหตุการณ์ในครั้งนี้อีกด้วย นอกจากนั้นความเสียหายทางอ้อมก็ยังเกิดตามมา อย่างเช่นในเรื่องของความเชื่อมั่น หรือร้านค้าผู้ให้บริการ ซึ่งไม่เคยที่จะรับทราบหรือเข้าไปเกี่ยวข้องอะไรด้วย แต่อาจจะทำการขึ้นเงินจากรายการใช้จ่ายผ่านบัตรเครดิตไม่ได้ หรือได้ช้าลง รวมทั้ง Bandwidth ของระบบเครือข่ายที่เพิ่มขึ้นจาก e-mail Phishing รวมถึงกระบวนการทำ Phishing ที่องค์การต้องรับเข้ามาทำให้สูญเสีย Bandwidth ของระบบเครือข่ายไปโดยไม่ก่อให้เกิดประโยชน์ใดๆ และแน่นอนว่าองค์การต้องหาระบบป้องกัน Phishing ซึ่งอาจจะพ่วงท้ายมากับระบบป้องกัน Spam แต่สุดท้ายแล้วทั้งหมดก็แปรกลับมาอยู่ในรูปของค่าใช้จ่ายที่องค์การต้องรับภาระเช่นเดียวกัน

ที่มาของ Phishing นั้น จริงๆ แล้วนี่เป็นเทคนิคหนึ่งในการล่อเหยื่อให้มาติดกับ โดยเพี้ยนมาจากคำว่า Fishing หรือการตกปลาที่ใช้เหยื่อล่อ โดยเหยื่อตัวจริงก็คือคนที่หลงเชื่อข้อความที่หลอกลวงตั้งแต่ต้นและตกเป็นเหยื่อส่งข้อมูลส่วนตัวให้กับ Phisher โดยถ้ามองให้ดีแล้วจะเห็นว่ารูปแบบของ Phishing ที่เรามักจะกล่าวถึงนั้นจะใช้วิธีการส่ง e-mail ที่มีหน้าตาเหมือนกับ e-mail จากผู้ให้บริการ หรือเปิด Web Site ที่มีหน้าตาเหมือนกับผู้ให้บริการจริง แล้วหลอกล่อให้เราไปใส่ข้อมูล ถ้าหากเป็นเมื่อก่อน หากเรามีเจตนาที่จะกรอกข้อมูลที่ไม่เป็นความจริงจะพบว่า Web Site ปลอมไม่สามารถตรวจสอบได้ แต่ในปัจจุบันด้วยเทคโนโลยีและวิธีการที่ซับซ้อนและชาญฉลาด ทำให้ทุกอย่างดูแนบเนียนเหมือนจริงมากยิ่งขึ้น แม้กระทั่งการกรอกข้อมูลที่ไม่เป็นความจริงลงไป Phisher ยังสามารถตรวจสอบได้ รวมถึงรูปแบบอื่นๆ ที่เพิ่มขึ้นมาจากเดิมซึ่งเป็นวิธีการที่มีมานานแล้วในต่างประเทศ แต่สำหรับในประเทศไทยอาจจะพึ่งเริ่มมี เพียงแต่ไม่มากเท่าใดนัก อาจจะเป็นเพราะว่าการสื่อสารในแง่ของ Internet ยังเติบโตอย่างค่อยเป็นค่อยไปในสมัยก่อน ผิดกับปัจจุบันที่มีการเติบโตรวดเร็วขึ้นเป็นเท่าตัว ดังนั้นการ Phishing ผ่านโทรศัพท์จึงเริ่มมีให้เห็นมากขึ้น เช่นการโทรศัพท์เข้ามาหา แล้วปลอมตัวว่าเป็นพนักงานจากธนาคารหรือองค์การบัตรเครดิตขอตรวจสอบข้อมูลหรือแม้แต่เป็นหน่วยงานทางด้านการเงินของภาครัฐเองก็ถูกแอบอ้าง ซึ่งก็มีคำพูดต่างๆ นานา พร้อมข้อมูลส่วนตัวของเราบางส่วนที่ทำให้เราหลงเชื่อว่านี่เป็นพนักงานของธนาคารหรือเจ้าหน้าที่ของภาครัฐจริงๆ โดยล่าสุดเมื่อผู้ให้บริการโทรศัพท์รายหนึ่งเปิดบริการเสริมไม่โชว์เบอร์ต้นทาง ยิ่งทำให้การตรวจสอบทำได้ยากขึ้น แม้ว่าบริการนี้จะมีข้อดีก็ตาม เพราะเป็นการรักษาความเป็นส่วนตัวของผู้โทรต้นทาง แต่ในทางกลับกันหากนำหมายเลขดังกล่าวไปใช้ทำ Phishing ผ่านโทรศัพท์ก็ยากจะที่ตรวจสอบได้เช่นเดียวกัน

สำหรับในส่วนของการป้องกัน หรือรับมือกับ Phishing นั้น ไม่มีวิธีใดที่สามารถป้องกันได้เต็มร้อยเปอร์เซ็นต์ เพราะแม้แต่มืออาชีพยังมีโอกาสโดนโจมตีได้เหมือนกัน แต่แทนที่จะตกใจหรือตื่นตัวไป วิธีป้องกันที่ดีที่สุดก็คือให้องค์การป้องกันเอาไว้ระดับหนึ่ง จากนั้นก็ขึ้นอยู่กับผู้ใช้แต่ละคนที่จะต้องระวังตัวเอง เพราะย่อมมี Phishing ส่วนหนึ่งที่หลุดรอดเข้ามาได้และที่เหลือก็ต้องมาตรวจสอบกันอีกที โดย e-mail Phishing นั้นจะมีขนาดและรูปร่างหน้าตาที่แตกต่างกันออกไป โดยบางครั้งจะดูเหมือนจริงมาก ในขณะที่บางครั้งกลับดูเหมือนเด็กเล่นเพราะมีการใช้ภาษาที่ค่อยสมเหตุสมผล

ขั้นตอนของ Phishing

กว่าที่เหยื่อจะถูกหลอกให้จะเข้าสู่การโจมตีแบบ Phishing ได้นั้น ผู้ที่ลงมือหรือ Phisher ทำจะต้องมีการวางแผนเสียก่อน โดยกระบวนการทั้งหมดแบ่งย่อยๆ เป็นขั้นตอนได้ดังนี้

1. ในขั้นแรกนั้น Phisher จะเริ่มวางแผนเสียก่อน โดยเลือกว่ากลุ่มธุรกิจใดที่เหมาะสมและควรเลือกเป็นเป้าหมายในการโจมตี ซึ่งส่วนใหญ่แล้วที่เห็นกันอยู่เป็นประจำก็คือ yahoo, Microsoft, Paypal, Hotmail, Citibank, MSN หรือถ้าหากเป็นการโจมตีภายในประเทศ ก็เช่น ธนาคารใหญ่ๆ หรือว่าองค์การชั้นนำ เป็นต้น จากนั้น Phisher จะตรวจสอบดูว่าจะทำอย่างไรจึงจะได้ e-mail Address ของลูกค้าในกลุ่มธุรกิจ หรือธนาคารดังกล่าว โดยอาจจะใช้ฐานข้อมูลลูกค้าที่ได้มาจากแหล่งต่างๆ ไม่ว่าจะเป็นการ Hack มา หรือซื้อมาจากตลาดมืด รวมทั้งอาจจะไปขโมยข้อมูลจากภายในธนาคารออกมาด้วยตัวเอง จากนั้นก็ใช้เทคนิคการส่ง e-mail ออกไปเป็นจำนวนมากๆ เช่นเดียวกับที่ใช้ส่ง e-mail Spam ทั้งนี้เพื่อส่ง e-mail Phishing ให้ลูกค้าธนาคารแห่งนั้น

2. ขั้นตอนต่อมาก็จะทำการ Setup ระบบ Web Site ปลอม โดยหลังจากเลือกธุรกิจที่ต้องการใช้เป็นเหยื่อล่อได้แล้ว รวมทั้งรู้แล้วว่าเหยื่อตัวจริงที่ต้องการเป็นใคร ต่อไปก็จะสร้าง Massage หรือข้อความซึ่งอยู่ในรูปของ e-mail ที่มีหน้าตาเหมือนของจริงบน Web Site ปลอม เพื่อใช้เก็บข้อมูล โดยอาจจะมีทั้งหน้า Web Page ที่เหยื่ออาจจะคลิกเข้าไปได้จริง รวมทั้งอาจจะมี e-mail ที่มีหน้าตาเหมือนจริงอีกด้วย ทั้งหมดนั้นมีการซ่อนข้อมูลจริงเอาไว้เพื่อป้องกันการตรวจสอบจากเหยื่อ

3. จะเป็นขั้นตอนที่เราพบกันอยู่เป็นประจำ เพราะขั้นตอนนี้ Phisher จะส่ง e-mail ทั้งหมดออกไปยังลูกค้าของธนาคารตามข้อมูลที่มีอยู่ ดังนั้น จึงไม่น่าแปลกว่าทำไมเราถึงคุ้นเคยกันขั้นตอนนี้ที่สุดและถ้าสังเกตให้ดีจะเห็นว่าบางครั้งเราอาจจะไม่ใช่ลูกค้าของธนาคาร หรือบริการแห่งนี้เสียด้วยซ้ำไป แต่กลับมี e-mail ส่งมาจากที่นั่นทำให้เราทราบได้ทันทีว่านี่เป็น e-mail Phishing อย่างแน่นอน ซึ่งหลังจากส่ง e-mail ไปแล้วและมีทั้งข้อความใน e-mail ที่สวยงามเหมือนของจริง รวมทั้งมี Web Site ปลอมแล้วก็ไม่ใช่เรื่องยากที่จะมีคนหลงกลคลิกเข้าไป ขั้นต่อไปก็แค่ทำระบบจัดเก็บข้อมูลของเหยื่อเท่านั้น โดยเหยื่อคนใดที่หลงเชื่อคลิกเข้าไปและกรอกข้อมูลลงไป ข้อมูลจะถูกบันทึกเอาไว้ทั้งหมดไม่ว่าจะเป็นบัญชีสำหรับการใช้บริการออนไลน์ไปจนถึงข้อมูลส่วนตัวและข้อมูลบัตรเครดิต ถ้าสังเกตให้ดีจะเห็นว่า Phisher ต้องการข้อมูลส่วนตัวเกือบทั้งหมดเพื่อสามารถปลอมตัวเป็นเหยื่อได้อย่างสมบูรณ์แบบ โดยรูปแบบดั้งเดิมที่ใช้กันได้ผลเสมอก็คือการหลอกให้ Verified Account เท่านี้ก็เรียบ-ร้อยแล้ว หลังจากนั้นข้อมูลจะถูกเก็บเอาไว้

4. เปลี่ยนจากสถานะ Phisher กลายเป็นอาชญากรคอมพิวเตอร์และสร้างอาชญากรรมอื่นๆ ต่อไป โดยจะเอาข้อมูลที่ได้จากการขโมยมานี้ไปใช้งานต่อ เช่น นำไปซื้อสินค้าและบริการ หรือทำสัญญาที่ส่งผลให้เจ้าของตัวจริงได้รับความเสียหายและจะมีการผลัดเปลี่ยนใช้งานต่อไปเรื่อยๆ ตราบใดก็ตามที่เจ้าของตัวจริงยังไม่สงสัย TPA news

อ่านต่อฉบับหน้า