Social Engineering

น.ต.ผศ. ดนัย ปฏิยุทธ
อาจารย์ฝ่ายศึกษา โรงเรียนนายเรือ

บทนำ

การโกงเพื่อให้ได้มาซึ่งข้อมูล ข่าวสาร ฯลฯ นั้นอาจจะกระทำได้หลากหลายวิธี เช่น Hacking, Cracking แต่วิธีอีกวิธีหนึ่งที่เป็นที่นิยมเช่นกันคือวิธีที่เรียกว่า Social Engineering

Social Engineering คือ วิธีการในด้านที่ไม่เกี่ยวกับเทคนิค ซึ่งเป็นศาสตร์และศิลป์ที่ผู้ประสงค์ร้าย (Cracker) ใช้หลอกผู้คน (แต่ไม่ใช่การควบคุมจิตใจหรือบังคับให้คนทำงานสิ่งใดเหนือไปจากพฤติกรรมที่ปรกติของเขาและมันไม่ใช่การหลอกที่ได้ผลร้อยเปอร์เซ็นต์ทุกครั้งไป) ให้เปิดเผย Password หรือข่าวสารอื่น ๆ ซึ่งข่าวสารเหล่านี้เมื่อตกอยู่ในมือผู้ประสงค์ร้ายเหล่านี้ จะทำให้ระบบต่าง ๆ เกิดความเสี่ยงต่อการถูกโจมตี โดย Social Engineering จะอาศัยหลักคือธรรมชาติของการชอบช่วยเหลือผู้คนอื่นและความอ่อนไหวของผู้คน โดยมักจะปลอมเป็นบุคคลที่ฟังดูน่าเชื่อถือ ลูกจ้างคนใหม่ ช่างซ่อม หรือนักวิจัย

จากการสำรวจพบว่าโดยเฉลี่ยใน ๑ วัน คนอเมริกันจะถูกชักจูงด้วยข้อความ ๑,๕๐๐ ข้อความจากโฆษณาภายในประเทศอย่างเดียว

ในปี ๑๙๙๘ ในจำนวนข่าวสารที่ส่งทาง E-mail ๗.๓ ล้านข้อความ จำนวน ๙๖% นับเป็น E-mail ขยะ (E-mail ที่มีแต่โฆษณาขายของ) และผู้คนได้รับ E-mail มากเป็นสองเท่า ของจำนวนที่เขาส่งในแต่ละวัน

ระดับ

ระดับของ Social Engineering มี ๒ ระดับ คือกายภาพ (Physical) เช่น ที่ทำงาน โทรศัพท์ ถังขยะ และจิตใจ (Psychological)

วิธีการ

การชักจูงคนอื่นให้คล้อยตามได้นั้นมี ๒ วิธีด้วยกันคือ

๑. ชักจูงโดยตรง เป็นการชักจูงที่กระทำได้ยาก เพราะต้องคิดก่อนตัดสินใจโดยการถามบุคคลนั้น ๆ เกี่ยวกับข้อมูลโดยตรง อาจจะได้ข้อมูลจากบุคคลแค่คนเดียวหรือข้อมูลจากหลาย ๆ คนแล้วนำมาประกอบเข้าด้วยกัน

๒. ชักจูงทางอ้อม เป็นการชักจูงที่กระทำได้ง่าย เพราะไม่ต้องคิดมาก (การไม่มีข้อขัดแย้งกับผู้ถามเป็นสิ่งที่ดี การให้ความร่วมมือจะได้รับมากกว่า ถ้าการเข้าถึงและการสอบถามไปในทางที่ละมุนละม่อม) เช่น การชักจูงโดยทำให้เกิดความรู้สึกอย่างมาก เช่น ความรู้สึกดีใจที่ถูกรางวัล

ปัจจัยที่มีผลต่อการชักจูงทางอ้อมมีดังต่อไปนี้

๑. *เจ้าหน้าที่ (Officer)*

บุคคลมักจะตอบสนองอย่างดีต่อบุคคลที่มีอำนาจหน้าที่ ตัวอย่างเช่น การวิจัยถึงการตอบสนอง ของพยาบาล ๒๒ คนใน Ward ต่าง ๆ ต่อคำสั่งของผู้ปลอมตัวเป็นนักกายภาพของโรงพยาบาล ในการให้ยา ๒๐ มิลลิกรัม แก่ผู้ป่วยใน Ward นั้น ๆ องค์ประกอบ ๔ อย่างที่พยาบาลควรจะถามบุคคลที่แอบอ้างเป็นนักกายภาพของโรงพยาบาล (แต่ไม่ถาม) คือ

- มาจากคำสั่งที่พยาบาลไม่เคยเห็นหน้าหรือพูดคุยก่อนเลย
- การสั่งจ่ายยาทางโทรศัพท์ ผิดนโยบายของพยาบาล
- ยานั้นไม่ได้อนุญาตให้ใช้ใน Ward นั้นๆ
- ยาที่ถูกสั่งจ่ายนั้นเป็นยาอันตรายและมีความแรงเป็น ๒ เท่า ของยาที่อนุญาตให้จ่ายในแต่ละวัน

แต่กระนั้นก็ตาม ๙๕% ของพยาบาลได้ทำตามผู้ที่แอบอ้างว่าเป็นนักกายภาพ

๒. *หายาก (Difficulty)*

ผู้คนมักจะตองสนองอย่างดี เช่น มีสิ่งบอกเหตุว่า สิ่งของเฉพาะนั้นๆ ที่เราต้องการมีจำนวนน้อย และจะขายเฉพาะช่วงนั้น ๆ ดอกเตอร์ Jack Brehm อาจารย์มหาวิทยาลัย สแตนฟอร์ด ได้ชี้ให้เห็นว่าบุคคลมักจะมีความปรารถนามากยิ่งขึ้น เมื่อเข้าใจว่าความอิสระในการได้รับสิ่งของนั้นมีจำกัด ยิ่งถ้ารู้ว่ามีบุคคลอื่นจ้องที่จะได้มาซึ่งครอบครองของสิ่งเดียวกัน ก็จะทำให้ปรารถนามากยิ่งขึ้นไปอีก

๓. *ความชอบและความคล้าย*

มักเป็นธรรมชาติที่มนุษย์มักชอบใครก็ตามที่คล้าย ๆ กับเรา บุคคลที่เกิดความชอบในกีฬา, ดนตรี, ศิลปะ หรือความสนใจอื่นๆ ที่คล้ายกัน ทำให้เราเจรจากับบุคคลนั้น ๆ ง่ายขึ้น และรู้สึกชอบเขาได้อย่างรวดเร็ว

๔. *ประโยชน์ซึ่งกันและกัน*

เป็นกฎของปฏิกิริยาในสังคมที่รู้กันเป็นอย่างแพร่หลายว่า เมื่อใครก็ตามที่ให้แก่เรา เราก็รู้สึกว่าต้องให้ตอบแทนแก่คน ๆ นั้น ถึงแม้ว่าสิ่งที่เขาให้เรานั้นอาจจะไม่เป็นที่ต้องการของอีกฝ่ายหนึ่ง แต่ก็ต้องตอบแทนตรง บางครั้งค่าตอบแทน อาจจะแพงกว่าที่เขาทำให้กับเรา

๕. การผูกมัดและความคงที่

สังคมจะให้ความสำคัญต่อความคงที่ในความประพฤติของบุคคล ถ้าเราสัญญาว่าจะทำสิ่งใดและไม่ได้กระทำตามสัญญา เราก็จะไม่ให้ความเชื่อถือคน ๆ นั้นอีกต่อไป ดังนั้นเราจึงต้องพยายามอย่างมากในการกระทำเพื่อให้คงที่กับการกระทำในอดีตเก่าก่อน ถึงแม้ว่าในอนาคตเราจะมองกลับมาและรู้สึกว่าสิ่งที่เราทำนั้นเป็นสิ่งที่โง่เขลา

๖. *การยอมรับของสังคม (Social Proof)*

ในสถานการณ์หลาย ๆ สถานการณ์ในสังคมไทยนั้น การจะตัดสินใจว่าการกระทำไหนสำคัญที่สุดให้ดูว่าคนอื่นที่อยู่ใกล้เรานั้นทำหรือพูดอย่างไร ซึ่งการกระทำแบบนี้เรียกว่า "Social Proof" ซึ่งเป็นกรรมวิธีที่ทำให้เรากระทำการใด ๆ ถึงแม้อาจจะขัดกับความสนใจของเรา โดยไม่ต้องเสียเวลาในการคิดในเชิงรุก

๗. การตัดสินใจตามกระแส (Go with the flow หรือ Conformity)

บางสถานการณ์ของสังคม การประพฤติปฏิบัติตนก็ต้องกระทำเพื่อไม่ให้คนอื่นเกลียดหรือดูโง่เขลาต่อหน้าฝูงชน โดยทำตามสิ่งที่คนในสังคมส่วนใหญ่กระทำกัน

๘. การกระจายความรับผิดชอบ (Diffusion of Responsibility)

ผู้ให้ข้อมูลจะไม่ลังเลและจะตอบถ้าตนเองรู้สึกว่าความรับผิดชอบของการให้ข้อมูลไม่ได้ตกที่ตนเองคนเดียว ตัวอย่างเช่น การที่ผู้หลอกบอกว่าคนอื่นๆ ได้ให้ข้อมูลที่ต้องการหมดแล้ว ก็จะทำให้ผู้ถูกถามลดความเครียดในการกรอกข้อมูล

๙. โอกาสในการประจบประแจง (Chance for Ingratiation)

การได้มีโอกาสได้กระทำการใด ๆ เพื่อให้ได้หน้าหรือผลงานเป็นที่ประจักษ์ต่อหัวหน้าหรือผู้บังคับบัญชาย่อมอยากที่จะกระทำสำหรับคนบางคน

๑๐. ภาระหน้าที่ทางศีลธรรม (Moral Duty)

สิ่งนี้เป็นสิ่งที่คนจะปฏิบัติตามเพราะเขารู้ว่าเป็นหน้าที่ทางศีลธรรมที่ต้องกระทำและเป็นส่วนหนึ่งของความรู้สึกผิด คนชอบที่จะหลีกเลี่ยงความรู้สึกผิดและถ้ามีโอกาสที่จะรู้สึกผิด เขาก็จะหลีกเลี่ยงไม่ให้มันเกิดขึ้นมา

๑๑. การมีส่วนร่วมแต่เก่าก่อน (Foot in the Door)

จากการวิจัยพบว่าคนจะปฏิบัติตามคำขอร้องที่ยิ่งใหญ่ถ้าหากในอดีตคนเคยได้ทำตามคำขอร้องที่เล็ก ๆ น้อย ๆ จากบริษัทเดียวกันนั้นมาก่อน

๑๒. การมีส่วนเกี่ยวข้องต่ำ (Low Involvement)

รปภ. คนทำความสะอาดหรือพนักงานต้อนรับ มักจะมีความเกี่ยวข้องน้อยกับระบบคอมพิวเตอร์ จึงคิดว่าตัวเองไม่ได้มีผลกระทบใด ๆ ต่อการร้องขอข้อมูล เขาจึงไม่วิเคราะห์ข้อดีหรือข้อเสียของการร้องขอข้อมูล ยิ่งไปกว่านั้นถ้า Social Engineer บอกเหตุผลดีๆประกอบเข้าไปด้วยโอกาสที่จะได้ข้อมูลก็มีมากขึ้นไปอีก

จุดอ่อน

สิ่งที่เสี่ยงต่อการถูกโจมตี คือ

๑. สมุดโทรศัพท์ เพราะสมุดโทรศัพท์ จะให้ชื่อ เบอร์โทรของคนที่เราจะปลอมเป็นคนนั้น ๆ
๒. แผนผังการทำงาน แผนผังการทำงานจะทำให้เราทราบว่า ใครอยู่ในตำแหน่งใดของบริษัทนั้น ๆ
๓. บันทึกช่วยจำ บันทึกช่วยจำจะให้ข่าวสารเกี่ยวกับการแสดงความเป็นตัวตนของผู้เขียน
๔. คู่มือของนโยบายบริษัท คู่มือนโยบายแสดงว่าบริษัทนั้นๆ มีความปลอดภัยหรือไม่
๕. ตารางการนัดหมาย ตารางการนัดหมายจะบอกว่า ลูกจ้างคนไหนจะอยู่หรือไม่อยู่ที่ทำงานในเวลานั้นๆ
๖. เหตุการณ์
๗. วันหยุดพักผ่อน
๘. ข่าวสาร ข่าวสารของข้อมูลที่สำคัญ เช่น Login, Password, Source code
๙. Hardware Hardware ที่ควรระวัง เช่น Hard Drive เก่า ๆ ไม่ใช้งานอาจจะถูกนำมา Restore เมื่อได้มาซึ่งข่าวสารที่มีประโยชน์ได้

เครื่องมือ

เครื่องมือที่ใช้ในการทำ Social Engineering มีดังนี้

๑. โทรศัพท์

๑.๑ ทั่วไป

เป็นเทคนิคที่ง่ายที่สุดของ Social Engineering มันจะเร็ว ไม่มีความเจ็บปวดและบุคคลที่ขี้เกียจก็สามารถกระทำได้ แค่โทรศัพท์ไปหาก็สามารถกระทำได้

๑.๒ อุปกรณ์ มีข้อควรพิจารณาดังนี้

๑.๒.๑ อุปกรณ์ Hardware คือโทรศัพท์ ซึ่งโทรศัพท์ที่ดีนั้นไม่ควรมี Call Waiting เพราะทำให้ดูไม่น่าเชื่อถือ โทรศัพท์ควรมีคุณภาพที่ดี Call ID ควรมี เพื่อที่จะโทรศัพท์กลับไปเบอร์ที่โทรมานั้น ๆ ได้

๑.๒.๒ Voice Changer ก็มีประโยชน์ เพราะการมีเสียงออกเด็ก ๆ ก็ฟังดูไม่น่าเชื่อถือ

๑.๒.๓ พยายามไม่ใช้ตู้โทรศัพท์ที่มีเสียง Background ดัง เพราะฟังดูไม่น่าเชื่อถือ ถ้าจะใช้โทรศัพท์สาธารณะ ให้พยายามใช้ตู้โทรศัพท์ที่เงียบ ๆ

๑.๓ เทคนิค มีข้อควรพิจารณาดังนี้

๑.๓.๑ ค้นหาเป้าหมาย เช่นต้องการหา Password เข้าสู่โครงข่ายของโรงเรียน เราก็โทรเข้าไปที่ศูนย์คอมพิวเตอร์ เราก็บอกว่า Account (ทราบมาก่อนแล้วหน้านี้) เราไม่สามารถเข้าไปได้เพราะลืม Password ก็ขอ Password ใหม่ ใช้ Voice Changer เป็นผู้หญิงก็ดี เพราะผู้ที่ทำหน้าที่ในการรับโทรศัพท์โดยส่วนใหญ่เป็นผู้ชาย

๑.๓.๒ โดยปกติก่อนที่เราจะโทรไปหลอกใคร ๆ นั้น เราต้องมีข้อมูลของคนที่เราจะสวมรอย เช่น มีเลขที่บัตรประจำตัว วันเดือนปีเกิด

๑.๓.๓ เมื่อเราปลอมสำเร็จแล้ว ให้ถามคำถามมากที่สุดเท่าที่จะหาได้ แต่ไม่ควรมากเกินไปเพราะอาจจะนำให้ถูกสงสัยได้

๑.๓.๔ เมื่อเราปลอมมาเป็นใครก็แล้วแต่ ให้พยายามฝึกพูดให้เหมือน เขา/เธอ ให้มากที่สุดเท่าที่จะมากได้ เช่น ถ้าเขา/เธอ พูดเสียงเหน่อ หรือคิดคำพูดใหม่ๆ ก็พยายามเลียนให้เหมือน วิธีดีที่สุด คือ โทรไปหาคนที่เราจะปลอมเป็นบุคคลนั้น ๆ เพื่อฟังเสียงและสไตล์การพูดของเขา

๑.๔ ตัวอย่าง ตัวอย่างของการหลอกในการสนทนา เช่น

“คุณได้โทรไปประเทศอียิปต์ ในช่วงหกชั่วโมงที่ผ่านมาไหม” ผู้หลอก ถาม

“ไม่” ชาวบ้านตอบ

“แต่เราตรวจพบว่าท่านใช้ไป ๒,๐๐๐ บาท ในการโทรน่ะครับและคุณก็ต้องจ่ายด้วยนะครับ”

“OK ผมจะช่วยคุณ โดยคุณบอกเบอร์สมาชิกของการโทรมาน่ะครับ แล้วผมจะลบบัญชีหนี้ให้”

๒. ไปรษณีย์

ผู้คนมักไม่ค่อยเชื่อถือใครก็ตามที่พูดคุยชักชวนตัวเราในการกระทำอะไรก็ตามทางโทรศัพท์ แต่ผู้คนจะเชื่อถือคำเขียนมากกว่า โดยมีข้อควรพิจารณาดังนี้

๒.๑ อุปกรณ์

แสตมป์ ซองจดหมาย แต่ถ้าจะดูให้น่าเชื่อถือ ต้องมีที่อยู่ให้ส่งกลับ

๒.๒ วิธีการปฏิบัติ

เอาที่อยู่ของผู้คนที่เราต้องการมา เพื่อใช้ส่งจดหมายไปให้โดยในจดหมายนั้น ๆ พยายามให้กรอกข่าวสารที่เราต้องการ เช่น เลขที่บัตรประจำตัวประชาชน โดยการกรอกพยายามทำให้อยู่ในรูปที่ง่าย

๓. อินเตอร์เน็ต

การ Hacking ต่างกับ Social Engineering ก็คือ Hacking จะใช้ข้อได้เปรียบในจุดอ่อนทางความปลอดภัย ส่วน Social Engineering จะใช้ข้อได้เปรียบในความจุดอ่อนของความรู้สึกนึกคิดของมนุษย์ และการเชื่อง่าย

๓.๑ การปฏิบัติ

๓.๑.๑ เช่นปลอมตัวเป็นผู้มีหน้าที่รับผิดชอบ ใน Chatroom ต่าง ๆ เพื่อให้ผู้คนมอบข้อมูลที่เราต้องการได้

๓.๑.๒ ส่ง E – mail ออกไปให้ผู้ใช้งานทุก ๆ คน (โดยหวังไว้ว่าคนใดคนหนึ่งของผู้ใช้งานจะตอบกลับมา) โดยบอกว่าเป็น System Administrator และต้องการ Password จากผู้ใช้งานโดยโกหกว่าจะใช้ในการทำงาน Admin. ซึ่งบุคคลที่ง่ายต่อการถูกหลอกก็คือ บุคคลที่เล่น Internet ใหม่ ๆ ที่ยังไม่รู้เล่ห์เหลี่ยมของบุคคลเหล่านี้ บางครั้งก็อาจใส่ Viruses, Worm, หรือ Trojan Horse ลงไปใน Attachment ของ E-mail เพื่อทำหน้าที่เป็น Backdoor ให้ผู้ประสงค์ร้ายเข้าไปในระบบภายหลัง

๓.๑.๓ วิธี “Frame – Spooting” คือการที่บุคคลสามารถใส่หน้า Web Site ลงไปบนอีกหน้า Web Site โดยไม่ได้รับอนุญาต คนที่เข้าไปเยี่ยม Web Site ที่ถูกใส่ Web Site ปลอม ก็อาจจะคัดลอกข้อมูลที่ถูกถามในหน้า Web Site นั้น ๆ

๓.๑.๔ วิธี “ Pump and Pump” คือ บุคคลในหน่วยงานที่ใช้วิธีหลากหลายเพื่อให้ผู้ลงทุนในเน็ตเกิดความสนใจในบริษัทและทำให้เกิดการ Pump (เพิ่ม) ค่าของราคาหุ้น จนกระทั่งสูงได้ระดับ บริษัทจึงขายหุ้นเพื่อให้ได้กำไร ซึ่งวิธี Pump and Pump จะใช้เทคนิคการอ้างสิทธิและวิธี Social Proof กล่าวคือการที่ผู้ส่งเสริมมูลค่าหุ้นร่วมมือกับบุคลากรในบริษัทจ่ายเงินให้นักเขียนในจดหมายแจ้งข่าวในอินเตอร์เน็ต เพื่อเขียนข่าวที่ดีในเชิงสร้างสรรค์หรือบางครั้งก็ทำถึงขั้นปล่อยข่าวลวง ให้แก่บริษัทให้ผู้ลงทุนเข้ามาอ่านและเข้าถึงข่าวสารนั้นๆ

๓.๑.๕ วิธี “Running Program” เป็นวิธีที่ผู้ประสงค์ร้ายส่ง Program มาให้ Run ทางอินเทอร์เน็ต (โดยอาจปลอมเป็น Admin.) โดยหลังจาก Run โปรแกรมนี้แล้ว Username และ Password ของผู้ใช้จะถูกส่งกลับไปให้ผู้ประสงค์ร้ายโดยอัตโนมัติ

๔. ด้วยตนเอง

๔.๑ อุปกรณ์

การแต่งกายจะต้องดูดี หวีผมให้เรียบร้อย สุภาพเรียบร้อย ติดบัตรประจำตัว ก็จะดูน่าเชื่อถือมากยิ่งขึ้น หรือไม่ก็บัตร Vision Pass

๔.๒ วิธีการปฏิบัติ

๔.๒.๑ เดินดูรอบ ๆ Office เพื่อหาข้อมูลตามโต๊ะทำงานต่าง ๆ

๔.๒.๒ ใช้วิธีทำเร็วกว่า “Shoulder Surfing” นั่นคือการมอง Password ผ่านไหล่ขณะที่คน ๆ นั้น พิมพ์ Password

๔.๒.๓ ขอใช้ Account คนอื่น

๔.๒.๔ ถาม Help Desk

เพราะบุคลากรที่มาทำงานที่ Help Desk นั้น จะไม่ค่อยมีความรู้เรื่องรักษาความปลอดภัยของข่าวสารข้อมูลมากนัก ดังนั้นเมื่อมีใครก็ตามมาถามเรื่องข้อมูล บุคลากร Help Desk ก็มักตอบหรือให้ข่าวสารนั้น ๆ ไป นอกจากนั้น Help Desk ยังถูกฝึกฝนมาให้เป็นมิตรไมตรีกับผู้คนและให้ข่าวสารต่าง ๆ แก่บุคคลที่เข้ามาสอบถาม

๔.๒.๕ ปลอมเป็นบุคคลอื่น เช่น ปลอมเป็นช่างซ่อม, หน่วยสนับสนุนสารสนเทศ, ผู้จัดการ, เพื่อนร่วมงานเพราะในบริษัทใหญ่ ๆ นั้น ลูกจ้างจะไม่รู้จักทุกคน บัตรประจำตัวก็สามารถปลอมได้

๔.๒.๖ Reverse Social Engineering (RSE) คือการปลอมเป็นบุคคลที่มีอำนาจหน้าที่และลูกจ้างจะต้องการข่าวสารจากเขา แต่วิธีนี้ต้องการการเตรียมตัวอย่างมาก เช่น RSE ประกอบด้วย การโจมตี (Sabotage), การโฆษณา (Advertising), การช่วยเหลือ (Assisting), ทำให้โครงข่ายมีปัญหาและโฆษณาว่าตัวเองคือผู้ที่สามารถช่วยเหลือได้ ขณะช่วยเหลือก็เอาข่าวสารจากสถานที่ทำงานนั้น ๆ

๔.๒.๗ Dumpster Diving หรือ Trashing นั่นคือการหาข่าวสารในถังขยะ ซึ่งบริษัทมักจะทิ้งข้อมูลต่าง ๆ ลงไปในถังขยะ เช่น สมุดโทรศัพท์ของพนักงานในแผนกต่าง ๆ แผนภูมิแสดงการจัดองค์กร บันทึกข้อความ คู่มือนโยบายของบริษัท ปฏิทินการนัดหมาย เหตุการณ์ที่เกิดขึ้นและวันหยุด คู่มือของระบบต่าง ๆ Source code ฮาร์ดแวร์ที่ไม่ต้องการใช้ รายชื่อ Login และ Password

วิธีป้องกัน

การป้องกันการ Social Engineering มีดังนี้

๑. สงสัยโทรศัพท์ที่ไม่ได้รับการเชื้อเชิญ ที่โทรมาถามข่าวสารเกี่ยวกับลูกจ้างหรือข่าวสารภายในบริษัท ถ้าใครก็ตามบอกว่ามาจากองค์กรใด พยายามพิสูจน์ความเป็นตัวตนที่แท้จริงของผู้ที่โทรมาถาม (โดยการสอบถามไปยังองค์กรที่ผู้โทรมานั้นบอกว่าทำงานอยู่)

๒. ไม่ให้ข่าวสารส่วนตัวหรือข่าวสารเกี่ยวกับองค์กรจนกว่าคุณจะได้รับรู้ตัวตนที่แท้จริงของบุคคลที่ต้องการข่าวสารนั้น

๓. ไม่บอกข่าวสารส่วนตัวหรือข่าวสารทางการเงินในอีเมล์และไม่ตอบอีเมล์ที่ถามข่าวสารพวกนี้

๔. ไม่ส่งข่าวสารที่สำคัญไปทางอินเทอร์เน็ตโดยปราศจากการตรวจสอบระดับของความปลอดภัยในการส่งข่าวสารของ Web Site นั้น ๆ

๕. พยายามสังเกต URL ของ Web Site ให้ดีเพราะ Web Site ที่ประสงค์ร้ายมักจะมี URL คล้ายกันมากกับ Web Site ที่มันจะหลอกลวงให้เหมือน
๖. ถ้าเราไม่แน่ใจว่าอีเมล์ที่ได้รับนั้นถูกต้องตามที่สมควรจะเป็นหรือไม่ ให้ทำการตรวจสอบโดยการติดต่อกับบริษัทที่อีเมล์นั้นกล่าวอ้างโดยตรง ไม่ใช่ข่าวสารที่แสดงในอีเมล์เพื่อการติดต่อ
๗. ติดตั้งซอร์ฟแวร์ ไฟร์วอล ตัวกรองอีเมล์ ให้กับระบบคอมพิวเตอร์เพื่อป้องกันอีเมล์ที่เข้ามาด้วยจุดประสงค์ร้าย
๘. System Admin. ต้องอบรมให้ความรู้แก่ User ของตัวเองเกี่ยวกับ Social Engineering
๙. พยายามทำให้ระบบคอมพิวเตอร์เป็นส่วนหนึ่งของงานของทุกคน ไม่ว่าเขาจะใช้คอมพิวเตอร์หรือไม่ก็ตาม

วิธีแก้ไข

เมื่อคุณถูกกระทำโดย Social Engineering วิธีการแก้ไขมีดังนี้

๑. ถ้าคุณคิดว่าได้เปิดเผยข้อมูลที่สำคัญเกี่ยวกับองค์กรของคุณ ให้รายงานเรื่องแก่บุคคลภายในองค์กรที่มีหน้าที่จัดการเกี่ยวกับปัญหานี้
๒. ถ้าคุณคิดว่าบัญชีด้านการเงินอาจถูกเปลี่ยนแปลงแก้ไข ติดต่อสถาบันการเงินของคุณและปิดบัญชีนั้น ๆ และคอยสังเกตการคิดค่าต่าง ๆ ต่อบัญชีของคุณ
๓. ถ้าเหตุการณ์ที่เกิดขึ้นรุนแรง แจ้งให้ตำรวจจัดการ
๔. ถ้ารู้ว่าถูก Social Engineering และได้บอก Password ไปแล้วด้วย ให้ทำการเปลี่ยน Password ใหม่โดยทันที

สรุป

สาเหตุที่ผู้คนใช้วิธี Social Engineering มากกว่าวิธีอื่น เช่น Hack ก็เพราะว่า ใช้ Social Engineering นี่ง่ายกว่า เพราะแค่โทรศัพท์ไปถามก็สามารถกระทำได้แล้ว โดยเทคนิคในด้านต่าง ๆ ของ Social Engineering นั้นไม่ว่าจะเป็นการแอบฟัง การดูเสมือนว่าไม่ทราบอะไร การดูน่าเชื่อถือของเจ้าหน้าที่ Social Engineering จะขึ้นอยู่กับการไม่มีความสามารถในการรู้เท่าทันวัฒนธรรมซึ่งขึ้นอยู่กับเทคโนโลยีสารสนเทศ นั่นคือไม่ทราบว่าข่าวสารที่รู้นั้นมีความสำคัญมาก เลยไม่ได้ระมัดระวังในการป้องกันข่าวสารนั้น จุดอ่อนที่เกิดจาก Social Engineering นี้จะเป็นการเกิดขึ้นทั่วไป เมื่อไม่รู้ ไม่แน่ใจว่าจะได้ข่าวสารโดยวิธี Social Engineering ก็ให้ทำท่าทางเป็นมิตรที่ดีกับผู้ที่ต้องการข่าวสารนั้นมาเพราะผู้คนทั่ว ๆ ไปมักจะเชื่อบุคคลทางโทรศัพท์และต้องการช่วย ถ้าบุคคลที่ถามนั้นทำตัวน่าเชื่อถือและบุคคลทั่ว ๆ ไปก็มักจะตอบสนองด้วยความสุภาพต่อผู้หญิง อาจจะยกย่อง ชมเชยหรือล้อเล่นบ้าง ก็อาจจะช่วย

ผู้ถูกถามให้อ่อนลง ไม่แข็งขืน ถ้าจนใจจริง ๆ ก็อาจพูดว่า “ผมสับสน ช่วยหน่อยน่ะครับ” แต่ Social Engineer ที่ดีก็จะรู้ว่าควรที่จะหยุดถามข่าวสารเมื่อใดก่อนที่ผู้ถูกถามจะรู้ตัว

สิ่งที่สำคัญที่สุดในการปกป้องการเกิด Social Engineering คือการไม่ให้ข่าวสารที่สำคัญแก่ใครก็ตามจนกระทั่งคุณแน่ใจแล้วว่าเขาคนนั้นคือใครก็ตามที่เขาบ่งบอกว่าเป็นและมีสิทธิและหน้าที่ที่สามารถเข้าถึงข่าวสารเหล่านั้น

ให้พยายามนึกอยู่เสมอว่า “คุณจ่ายเงินมากมายเพื่อซื้อเทคโนโลยีและการบริการ แต่โครงสร้างของโครงข่ายก็ยังมีจุดอ่อนต่อการถูกโจมตีเสมอ”

อ้างอิง

๑. http://www.morehouse.org/hin/blckcrwl/hack/soceng.txt

๒. http://www.us-cert.gov/cas/tips/ST04-014.html