"La Ingeniería Social: El Arte del Engaño"

El principio en el que se sustenta la Ingeniería Social es aquel que afirma que en cualquier sistema los usuarios y el personal son el eslabón débil de la cadena. En la práctica, un Ingeniero Social utiliza comúnmente el teléfono o internet para engañar a gente simulando, por ejemplo, ser un empleado de un banco o de una empresa, un compañero de trabajo, un técnico o un cliente y así obtener información de una persona o empresa.

En otras palabras, es el arte de persuadir con engaño para que casi sin darse cuenta, los afectados compartan datos vitales con un desconocido. De acuerdo a Christopher Hadnagy en su libro "Ingeniería Social el Arte del Hacking Personal" se define a la Ingeniería Social como "El acto de manipular a una persona para que lleve a cabo una acción que -puede ser o no- lo más conveniente para cumplir con cierto objetivo. Este puede ser la obtención de información, conseguir algún tipo de acceso o logar que se realice una determinada acción". Por ejemplo, los médicos, los psicólogos y los terapeutas a menudo utilizan elementos que se consideran de Ingeniería Social para "manipular" a sus pacientes para que realicen acciones que son buenas para ellos, mientras que un estafador utiliza elementos de la Ingeniería Social para convencer a su víctima para que realice acciones que le perjudican. Aunque el resultado es muy diferente, el proceso puede ser muy parecido.

Otras definiciones de ingeniería Social:

"La Ingeniería Social es mentir a la gente para obtener información".

"La Ingeniería Social es ser un buen actor".

"La Ingeniería Social es saber cómo conseguir cosas gratis".

Wikipedia la define como el "acto de manipular a la gente para llevar a cabo acciones o divulgar información confidencial. Aunque parecido a una estafa o un simple fraude, el término se aplica normalmente a las artimañas o engaños con el propósito de obtener la información, llevar a cabo un fraude o acceder a un sistema informático; en la mayoría de los casos, el atacante nunca se enfrenta cara a cara con la víctima".

El diccionario de Webster define "social" como "relativo o perteneciente a la vida, el bienestar y las relaciones de los seres humanos en una comunidad". También define la "ingeniería" como el "arte o la ciencia de llevar a aplicación práctica el conocimiento de las ciencias puras como la física o la química, en la construcción de máquinas, puentes, edificaciones, minas, embarcaciones y plantas químicas o artilugios ingeniosos; maniobrar".

Combinando ambas definiciones se puede ver fácilmente que la Ingeniería Social es el arte, o mejor aún, la ciencia, de maniobrar hábilmente para lograr que los seres humanos actúen de cierta forma en algún aspecto de sus vidas.

La Ingeniería Social es utilizada en la vida diaria, por ejemplo, en la manera en que los niños consiguen que los padres atiendan a sus peticiones. Es utilizada por los profesores en el modo de interactuar con sus estudiantes y por los doctores, abogados o psicólogos para obtener información de sus pacientes o clientes.

En definitiva, es utilizada en cualquier interacción humana, desde los niños hasta los políticos.

La Ingeniería Social no es una acción resuelta, sino una recopilación de las habilidades que, cuando se unen, componen la acción, el ingenio y la ciencia a la cual se le llama Ingeniería Social. De la misma manera, una buena comida no es sólo un ingrediente, sino que se crea con la mezcla cuidadosa de varios ingredientes. Podría decirse que un buen Ingeniero Social es como un chef.

La Ingeniería Social y su lugar en la sociedad

La Ingeniería Social puede utilizarse en muchas facetas de la vida, pero no todos estos usos son maliciosos o negativos. Muchas veces la Ingeniería Social puede utilizarse para motivar a una persona para realizar una acción que es buena para ella: ¿Cómo?

Piense en esto: Juan necesita perder peso. Sabe que su salud es mala y que tiene que hacer algo al respecto. Todos los amigos de Juan tienen sobrepeso también. Incluso hacen chistes sobre las alegrías de tener sobrepeso y dicen cosas como "me encanta no tener que preocuparme por mi figura". Por una parte, esto es un aspecto de la Ingeniería Social. Es

una prueba social o consenso, donde lo que se considera aceptable está determinado por quienes están alrededor. Sin embargo, si uno de los amigos de Juan pierde peso y en vez de criticar a los demás decide intentar ayudarlos, existe la posibilidad de que cambie la estructura mental de Juan sobre su peso y empiece a pensar que adelgazar es posible y bueno para él.

Esto es, en esencia, Ingeniería Social. A continuación, otros ejemplos:

1.- El Timo 419: Llamado también la Estafa Nigeriana, se lleva a cabo principalmente por correo electrónico no solicitado. Adquiere su nombre del número de artículo del código penal de Nigeria que viola, ya que buena parte de estas estafas provienen de ese país.

Si recibe algo de correo basura, con mucha seguridad ya debe haber recibido un e-mail en inglés donde la explica que cierto funcionario que tiene acceso a unos fondos acumulados pero que tiene problemas para efectuar él mismo la operación, porque se trata de fondos secretos y como tiene que sacarlo de Nigeria lo más rápido posible, entonces ofrece una compensación fuera de lo común.

Los defraudadores profesionales ofrecen transferir millones de dólares a su cuenta bancaria a cambio de un pequeño cargo. Si usted responde al ofrecimiento inicial, es posible que reciba documentos que parecen ser oficiales. Entonces, generalmente se le pide que provea los números de sus cuentas bancarias y una serie de información de carácter privado para hacer efectivo el traspaso.

Por increíble que parezca, en el año 2001 alrededor de 2.600 ciudadanos fueron víctimas de esta estafa, con una pérdida de más de $300.000 dólares.

2.- Robo de empleados:

El tema de robo de empleados puede llenar volúmenes enteros. Más del 60% de los empleados entrevistados admitieron haber tomado información de algún tipo de sus empleadores. Muchas veces esta información se vende a la competencia. Otras veces, lo que roban los empleados es tiempo o recursos; en algunos casos, un empleado descontento puede causar mucho daño.

Caso:

Cierta empresa consideraba que todo el mundo allí era parte de la "familia" y que no era necesario aplicar políticas de despido de empleados. Desgraciadamente llegó el día de despedir a uno de los directivos de más alto rango de esta empresa. El despido fue amigable y el directivo fue comprensivo. Una cosa que la empresa hizo correctamente fue llevar el despido a la última hora de la jornada para evitar el bochorno o cualquier tipo de distracción. Hubo un apretón de manos y entonces el ex directivo hizo la fatídica pregunta: ¿Puedo tomarme una hora para limpiar mi mesa y sacar algunas fotos personales del computador?

Al tener buenas sensaciones después de la reunión todos estuvieron rápidamente de acuerdo y se fueron entre alegres sonrisas. Entonces el ex directivo se fue a su despacho, empaquetó sus objetos personales, sacó las fotos y otros datos de su computador, se conectó a la red y limpió el equivalente a 11 servidores en información: registros de contabilidad, nóminas, facturas, órdenes, historiales, gráficos y mucho más, todo borrado en cuestión de minutos. El ex directivo abandonó el edificio sin dejar pruebas de que él fue quien llevó a cabo este ataque.

Un empleado descontento al que se deja actuar libremente puede ser más devastador que un equipo de hackers decididos y experimentados. La pérdida estimada sólo en empresas de Estados Unidos por robos de empleados es del orden de 15.000 millones de dólares.

3.- Phishing:

Un ataque muy simple pero efectivo es engañar al usuario llevándolo a pensar que un administrador del sistema le está pidiendo una contraseña para propósitos legítimos. Quienes navegan en internet frecuentemente reciben mensajes que solicitan contraseñas o información de su tarjeta de crédito con el motivo de crear una cuenta, reactivar una configuración u otra operación aparentemente inofensiva. A este tipo de ataques se lo llama *phishing*. Los usuarios de estos sistemas deberían ser advertidos temprana y frecuentemente para que no divulguen contraseñas u otra información sensible a personas que dicen ser administradores.

4.- Spoofing:

Técnicas de suplantación de identidad en la red generalmente con usos maliciosos. Por ejemplo, a fuerza de haber sufrido virus gracias a correos engañosos, bloqueos de casillas a causa del spam y otras delicias, muchos usuarios sólo chequean el correo electrónico proveniente de remitentes conocidos y "seguros". Esta (última) opción también se ve amenazada gracias al spoofing, técnica que puede engañar a cualquier usuario enviando e-mails de todo tipo (propaganda, agitación política, etc.) bajo la máscara de una dirección "segura" de un remitente conocido.

En este caso, alguien se apropia del nombre y la contraseña de una dirección de correo y la utiliza para enviar correo masivo preferentemente a las personas que no dudarían en abrir una mensaje proveniente de esa dirección (dato fácilmente extraíble de la lista de correo).

Los distintos tipos de Ingenieros Sociales

La Ingeniería Social puede adoptar muchas formas. Como lo habíamos dicho anteriormente, Puede ser maliciosa o amigable puede crear o destruir. Es por ello que existen diferentes tipos de Ingenieros Sociales:

- Hackers.
- Probadores de seguridad.
- Espías.
- Ladrones de identidad.
- Empleados descontentos.
- Artistas del timo.
- Agentes de recursos humanos.
- Vendedores.
- Gobiernos: No siempre son vistos como Ingenieros Sociales, pero los gobiernos utilizan la Ingeniería Social para controlar el mensaje que envían a las personas que gobiernan.
- Médicos, Psicólogos, Abogados.

Parece que se puede encontrar la Ingeniería Social o algún aspecto de ella en cualquier campo. Por eso, se sostiene firmemente que la Ingeniería Social es una ciencia.

El Entorno Conceptual de la Ingeniería Social y Cómo Utilizarlo

El conocimiento es poder, cierto. En este sentido, la formación es la mejor defensa contra la mayoría de los ataques de Ingeniería Social. Incluso en aquellos contra los que el conocimiento no puede protegerle al100%, conocer en detalle estos ataques le mantendrá alerta. La formación puede ayudarle a mejorar sus propias habilidades y a estar vigente.

No obstante, además de formación, necesita práctica.

Recopilar Información

Se dice que no hay información irrelevante. En términos de Ingeniería Social, hasta el menor detalle puede conducir a una brecha beneficiosa para el éxito de sus propósitos.

Caso:

Se desea acceder a una empresa que apenas tiene rastro en internet. Ya que la empresa tiene muy pocas vías por las que penetrar, conseguir acceder a ella constituye un auténtico reto.

Primero se comenzó barriendo Internet en busca de algún detalle que conduzca a un camino de entradas. En una de las búsquedas se localizó a un alto directivo de la empresa que utilizaba su correo electrónico corporativo en un foro de coleccionista de sellos. Rápidamente, el recopilador registró una URL similar a www.stampcolletion.com y buscó unas cuantas fotos de sellos antiguos en Google. Creó un sencillo sitio web para mostrar su "colección de sellos" y después envió un correo electrónico al directivo de la empresa:

"Estimado Señor:

He visto en www.forum.com que le interesan los sellos de los años cincuenta. Mi abuelo falleció recientemente y me dejó una colección

de sellos que me gustaría vender. He creado un sitio para tal efecto. Si quisiera ver la colección, visite por favor www.stampcollection.com."

Antes de enviar el correo electrónico al objetivo, quería asegurarse de lograr el máximo impacto. Consiguió el número de teléfono del directivo a través del foro y le dejó un mensaje en el buzón de voz: *"Buenos días señor. Vi su mensaje en www.forum.com. Mi abuelo acaba de fallecer y me ha dejado unos cuantos sellos de los años 50 y 60. He hecho unas fotos y he creado un sitio web. Si está interesado puedo enviarle un vínculo para que eche un vistazo"*.

El directivo estaba ansioso por ver la colección y aceptó de buena gana el correo. El recopilador de información le envió el correo y esperó que hiciera un clic en el vínculo. Lo que hizo el recopilador, fue incrustar un marco malicioso en el sitio web. Este marco contenía un código que explotaría una vulnerabilidad, muy conocida entonces, del navegador Internet Explorer y daría al recopilador control sobre todo el computador del directivo.

La espera no duró mucho tiempo. En cuanto el directivo recibió el correo, hizo clic en el vínculo poniendo a su empresa en peligro.

Una minúscula cantidad de información (el correo electrónico que utilizaba el directivo para buscar sellos) fue lo que condujo a la situación de peligro. Ninguna información es irrelevante. Con esa idea en mente, surgen algunas preguntas en relación a la recopilación de información:

- ¿Cómo se puede recopilar información?
- ¿Qué fuentes de recopilación de información existen para Ingenieros Sociales?
- ¿Qué puede deducir de esos datos para retratar a sus objetivos?
- ¿Cómo puede localizar, almacenar y catalogar toda esta información para facilitar su utilización?

Un área excelente para la recopilación de información es la de ventas. Los vendedores suelen ser muy habladores y fáciles de tratar suelen ser muy buenos reuniendo información sobre aquellos con quienes interactúan.

Recopilar información es como construir una casa. Si intenta empezar por el tejado, lo más probable es que fracase. Una buena casa se construye empleando unos cimientos sólidos y edificando a partir de ahí, del suelo hacia arriba. Al recopilar información una persona puede sentirse abrumada intentando organizar y utilizar el material, por lo que es buena idea crear un archivo o iniciar una aplicación de recopilación para reunir datos.

Existen muchas herramientas que ayudan a recopilar y utilizar la información. Para realizar pruebas de seguridad y auditorías de Ingeniería Social es recomendable la utilización de una distribución de Linux llamada BackTrack específicamente diseñada con este propósito. BackTrack, como casi todas las distribuciones de Linux, es de software libre y fuente abierta. Quizás su mayor ventaja sea que contiene más de 300 herramientas diseñadas para ayudar en auditorías de seguridad.

Dos instrumentos de BackTrack especialmente útiles para la recopilación y almacenaje de información son Dradis y BasKet.

Para un Ingeniero Social, reunir información es la clave de cada actuación, pero si no se puede recuperar y utilizar información rápidamente, entonces resulta inútil. Una herramienta como BasKet hace que guardar y utilizar datos sea muy sencillo.

Aunque BasKet es una gran herramienta, si hace mucha recopilación de información o si trabaja en equipo y necesita reunir, guardar y utilizar los datos, entonces es importante tener una herramienta que permita compartir la información por varios usuarios. Esta herramienta es Dradis.

Este programa es una aplicación web independiente que proporciona un almacén centralizado de la información que se ha reunido y un medio a partir del cual planificar los siguientes pasos.

Pensar como un Ingeniero Social

Caso:

"En una ocasión arrendé un auto para hacer un viaje de negocios. Mi acompañante y yo cargamos nuestro equipaje en el maletero; cuando entramos en el auto reparamos en una pequeña bolsa de basura que había atrás. La persona que iba conmigo dijo: *Este servicio va de mal*

en peor. Se supone que por lo que pagamos podrían al menos limpiar el coche.

Es cierto, sería lógico, pero antes de que tirara la bolsa al basurero más cercano, dije: *Déjame echar un vistazo rápido.* Cuando abrí la bolsa y aparté los envoltorios lo que encontré allí, me pareció a simple vista impactante: era la mitad de un cheque partido. Inmediatamente volqué el contenido de la bolsa y encontré un recibo del banco y la otra mitad del cheque. Una vez pegado con cinta, el cheque revelaba el nombre de la persona, la empresa, su número de teléfono, número de cuenta bancaria y el código de identificación bancaria. Por suerte para el propietario de estos datos, no soy una mala persona porque sólo se necesitan un par de pasos más para cometer un robo de identidad.

Esta historia personifica la relación que tiene la gente con su información valiosa. Esta persona que arrendó el auto antes que yo y después, al tirar el cheque, estaba convencido de que lo que había hecho desaparecer de forma segura".

Fuentes de Recopilación de Información

Existen muchas fuentes diferentes de recopilación de información. La siguiente lista no puede abarcar todas las posibilidades existentes, pero perfila las opciones más importantes.

1.- Recopilar Información de los sitios web

Los sitios web personales o corporativos pueden proporcionar una gran cantidad de información. Lo primero que hará normalmente un buen Ingeniero Social es reunir todos los datos que pueda del sitio web de la persona o de la empresa. Dedicarle tiempo al sitio web puede llevarle claramente a:

- Lo que hacen.
- Los productos y servicios que ofrecen.
- Las localizaciones físicas.
- Las ofertas de puestos de trabajo.

- Los números de contacto.
- Las biografías de los ejecutivos o del consejo administrativo.
- El foro de apoyo.
- La nomenclatura de los correos electrónicos.
- Palabras o frases especiales que pueden ayudar a determinar contraseñas.

2.- Servidores Públicos

Los servidores públicos de una empresa también son buenas fuentes de la información que sus sitios web no proporcionan.

Las direcciones IP pueden decir si los servidores están alojados localmente o con un proveedor, con los registros de DNS puede determinar nombres y funciones de servidores y direcciones IP.

3.- Redes Sociales

Muchas empresas han empezado a interesarse por las redes sociales. Es publicidad barata que llega a un gran número de clientes potenciales. También es una nueva corriente de información de una empresa que puede proporcionar algunos datos útiles.

Caso:

"El presidente de Hewlett- Packard reveló más que su jerarquía laboral cuando mencionó la iniciativa de almacenamiento en la web de la firma fabricante de computadoras en su perfil de LinkedIn.

En un descuido, alertó a sus competidores sobre detalles que no se habían difundido antes respecto de los servicios de cloud computing de la marca. La información se retiró más tarde, si bien no antes de que los rivales pudieran ver los planes.

Conforme los empleados brindan más información online sobre su vida, desde actualizaciones sobre su situación, controles de ubicación y cambios en el currículum, los empleadores corren más riesgos de que los competidores observen todos sus movimientos.

En una encuesta de Forrester Research del año pasado entre más de 150 compañías que monitorean medios sociales, más del 82% expresó que usaba esos datos para inteligencia competitiva".

4.- Sitios de usuarios blogs y otros

Los sitios de usuarios como los blogs, wikis y videos online no solo pueden proporcionar información sobre la empresa objetivo, sino que también ofrecen una conexión más personal a través del contenido subido por el usuario. Un empleado descontento que está hablando en su blog sobre sus problemas en la empresa, puede ser susceptible de compartir información privilegiada que cualquiera puede ver y leer.

Un buen ejemplo es esta web www.icanstalku.com Al contrario de lo que indica su nombre "puedo acosarte", no anima a la gente a acosar a otros. Este sitio pone de manifiesto el total descuido de muchos usuarios de Twitter. Rastrea el sitio de Twitter y busca usuarios que son tan imprudentes como para colgar fotos hechas con sus teléfonos Smartphone. Mucha gente no sabe que la mayoría de los Smartphone incrustan datos de localización en sus fotos. Cuando un usuario cuelga una foto en la web con esta información incrustada, puede conducir a una persona hasta su localización.

Fuente:

Ingeniería Social. El Arte del Hacking Personal, Christopher Hadnagy.

Ethical hacking, las técnicas de los hacker al servicio de la seguridad, Manuales Users.

Diario La Segunda, Edición Lunes 26 de Septiembre de 2011.