Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

INGENIERÍA SOCIAL: CORROMPIENDO LA MENTE HUMANA

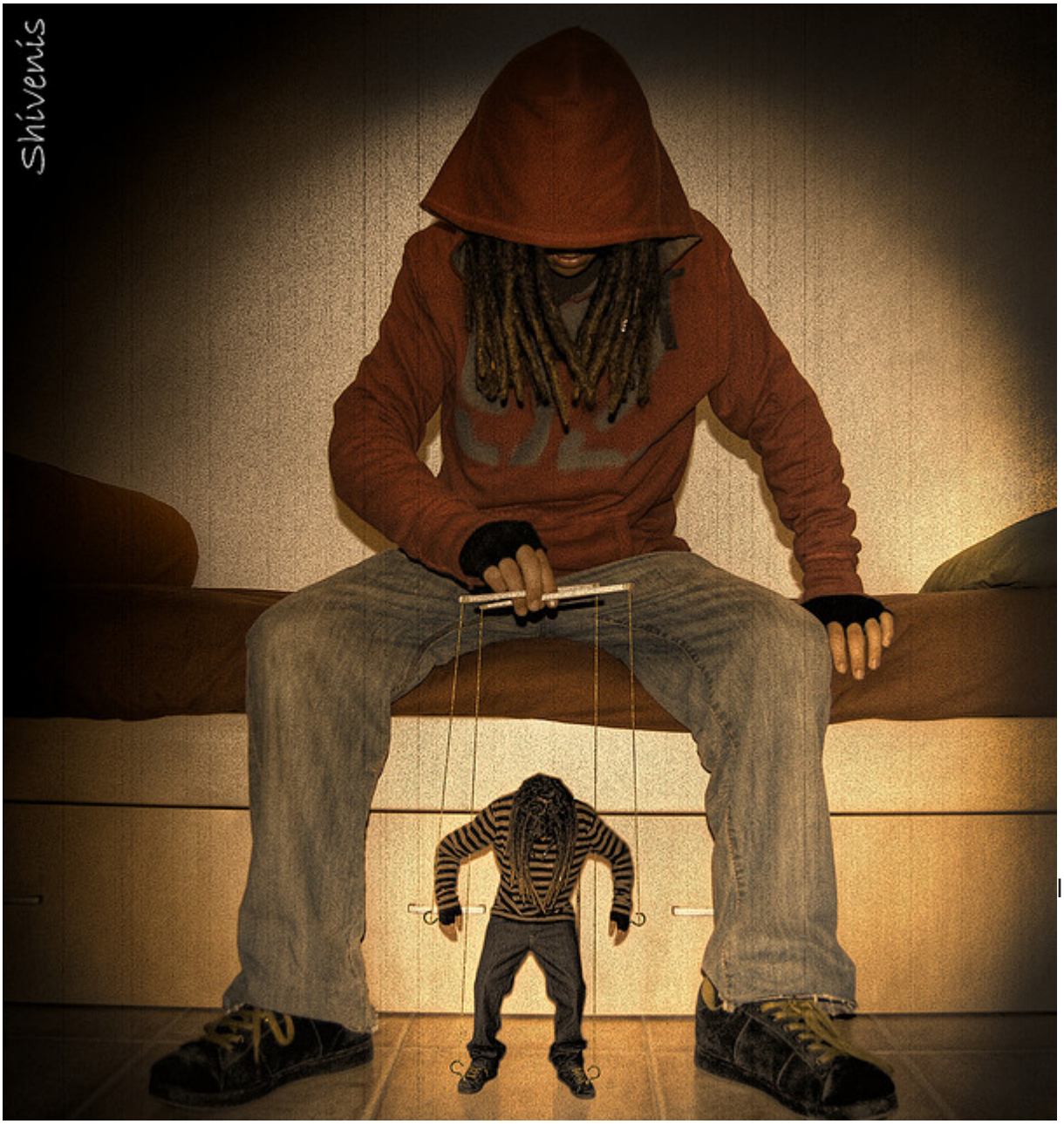
Edgar Jair Sandoval Castellanos

amenaza

numero-10

INTRODUCCIÓN

Hoy en día, uno de los activos más valiosos para las organizaciones es la información. Compartir información con otras entidades, sugiere la mayoría de las veces una invasión de la privacidad.



llo, las instituciones (gubernamentales, educativas, financieras, etc.) buscan la manera de implementar controles de seguridad para proteger su información, como circuitos de cámaras, cajas fuertes, firewalls, etc., medidas que además resultan costosas.

Sin embargo, hay un recurso inseguro que almacena información muy sensible: la mente humana. Ya sea por olvido o por el reto que implica asegurar la información dentro de las cabezas de sus empleados, las organizaciones no le prestan mucha atención a este aspecto.

Sin importar cuántos candados físicos o lógicos haya para proteger un activo, al dar acceso a una persona, siempre existirá un riesgo humano presente, y por tanto, vulnerable a ingeniería social.

Img 1. Cortesía Flickr

¿Qué es la Ingeniería Social?

La Ingeniería Social es el acto de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Éstas contemplan entre otras cosas: la obtención de información, el acceso a un sistema o la ejecución de una actividad más elaborada (como el robo de un activo), pudiendo ser o no del interés de la persona objetivo.

La Ingeniería Social se sustenta en un sencillo principio: “el usuario es el eslabón más débil”. Dado que no hay un solo sistema en el mundo que no dependa de un ser humano, la Ingeniería Social es una vulnerabilidad universal e independiente de la plataforma tecnológica. A menudo, se escucha entre los expertos de seguridad que la única computadora segura es la que esté desenchufada, a lo que, los amantes de la Ingeniería Social suelen responder que siempre habrá oportunidad de convencer a alguien de enchufarla[1].

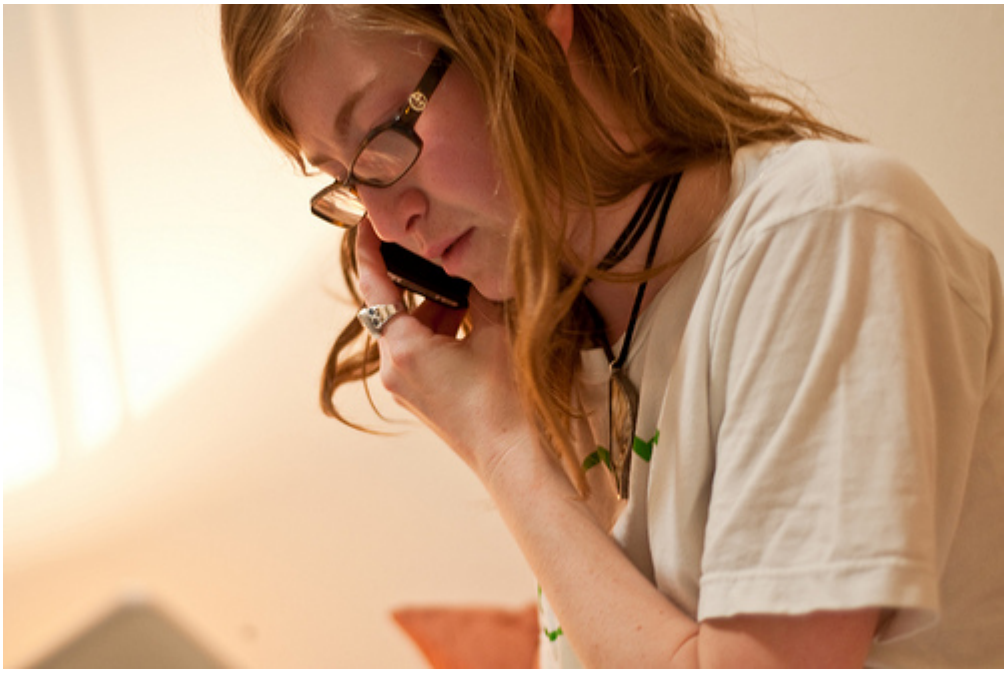
La Ingeniería Social es un arte que pocos desarrollan debido a que no todas las personas tienen “habilidades sociales”. Aún así, hay individuos que desde pequeños han demostrado tener la aptitud y con un poco de entrenamiento convertirla en el camino ideal para realizar acciones maliciosas. Por ejemplo, hay *crackers* que en vez de perder horas rompiendo una contraseña, prefieren conseguirla preguntando por teléfono a un empleado de soporte técnico.

FORMAS DE ATAQUE

Las formas de ataque son muy variadas y dependen de la imaginación del atacante y sus intereses. En general, los ataques de Ingeniería Social actúan en dos niveles: el físico y el psicosocial. El primero describe los recursos y medios a través de los cuales se llevará a cabo el ataque, y el segundo es el método con el que se engañará a la víctima.

Las formas usadas a nivel físico son:

- Ataque por teléfono. Es la forma más persistente de Ingeniería Social. En ésta el perpetrador realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, como un técnico de soporte o un empleado de la misma organización. Es un modo muy efectivo, pues las expresiones del rostro no son reveladas y lo único que se requiere es un teléfono.



Img. 2 Cortesía Flickr

- Ataque vía Internet. Desde que Internet se volvió uno de los medios de comunicación más importantes, la variedad de ataques en red se incrementaron tanto como la gran cantidad de servicios que existen en él. Los ataques más comunes son vía correo electrónico (obteniendo información a través de un phishing o infectando el equipo de la víctima con malware), web (haciendo llenar a la persona objetivo un formulario falso) o inclusive conversando con personas específicas en salas de chat, servicios de mensajería o foros.

- *Dumpster Diving* o *Trashing* (zambullida en la basura). Consiste en buscar información relevante en la basura, como: agendas telefónicas, organigramas, agendas de trabajo, unidades de almacenamiento (CD's, USB's, etc.), entre muchas otras cosas.

Img. 3 Cortesía Flickr

- Ataque vía *SMS*. Ataque que aprovecha las aplicaciones de los celulares. El intruso envía un mensaje *SMS* a la víctima haciéndola creer que el mensaje es parte de una promoción o un servicio, luego, si la persona lo responde puede revelar información personal, ser víctima de robo o dar pié a una estafa más elaborada.

- Ataque vía correo postal. Uno de los ataques en el que la víctima se siente más segura, principalmente por la fiabilidad del correo postal. El perpetrador envía correo falso a la víctima, tomando como patrón alguna suscripción de una revista, cupones de descuento, etc. Una vez que diseña la propuesta para hacerla atractiva, se envía a la víctima, quien si todo sale bien, responderá al apartado postal del atacante con todos sus datos.

- Ataque cara a cara. El método más eficiente, pero a la vez el más difícil de realizar. El perpetrador requiere tener una gran habilidad social y extensos conocimientos para poder manejar adecuadamente cualquier situación que se le presente. Las personas más susceptibles suelen ser las más “inocentes”, por lo que no es un gran reto para el atacante cumplir su objetivo si elige bien a su víctima.

Por otro lado, existen entornos psicológicos y sociales que pueden influir en que un ataque de ingeniería social sea exitoso. Algunos de ellos, son:

- “*Exploit* de familiaridad”. Táctica en que el atacante aprovecha la confianza que la gente tiene en sus amigos y familiares, haciéndose pasar por cualquiera de ellos. Un ejemplo claro de esto ocurre cuando un conocido llega a una fiesta con uno de sus amigos. En una situación normal nadie dudaría de que ese individuo pudiera no ser de confianza. Pero ¿de verdad es de fiar alguien a quien jamás hemos tratado?

- Crear una situación hostil. El ser humano siempre procura alejarse de aquellos que parecen estar

locos o enojados, o en todo caso, salir de su camino lo antes posible. Crear una situación hostil justo antes de un punto de control en el que hay vigilantes, provoca el suficiente estrés para no revisar al intruso o responder sus preguntas.

rev10_ingesoc_img4

Image not found or type unknown

Img. 4 Cortesía Flickr

- Conseguir empleo en el mismo lugar. Cuando la recompensa lo amerita, estar cerca de la víctima puede ser una buena estrategia para obtener toda la información necesaria. Muchas pequeñas y medianas empresas no realizan una revisión meticulosa de los antecedentes de un nuevo solicitante, por lo que obtener un empleo donde la víctima labora puede resultar fácil.
- Leer el lenguaje corporal. Un ingeniero social experimentado puede hacer uso y responder al lenguaje corporal. El lenguaje corporal puede generar, con pequeños, detalles una mejor conexión con la otra persona. Respirar al mismo tiempo, corresponder sonrisas, ser amigable, son algunas de las acciones más efectivas. Si la víctima parece nerviosa, es bueno reconfortarla. Si está reconfortada, ¡al ataque!
- Explotar la sexualidad. Técnica casi infalible. Las mujeres que juegan con los deseos sexuales de los hombres, poseen una gran capacidad de manipulación, ya que el hombre baja sus defensas y su percepción. Probablemente suene asombroso, pero es aprovechar la biología a favor.

¿CÓMO DEFENDERSE CONTRA LA INGENIERÍA SOCIAL?

La mejor manera de enfrentar el problema, es concientizar a las personas al respecto. Educarles sobre seguridad y fomentar la adopción de medidas preventivas. Otros mecanismos sugeridos son:

- Nunca divulgar información sensible con desconocidos o en lugares públicos (como redes sociales, anuncios, páginas web, etc.).
- Si se sospecha que alguien intenta realizar un engaño, hay que exigir se identifique y tratar de revertir la situación intentando obtener la mayor cantidad de información del sospechoso.
- Implementar un conjunto de políticas de seguridad en la organización que minimice las acciones de riesgo.
- Efectuar controles de seguridad física para reducir el peligro inherente a las personas.
- Realizar rutinariamente auditorías y *pentest* usando Ingeniería Social para detectar huecos de seguridad de esta naturaleza.
- Llevar a cabo programas de concientización sobre la seguridad de la información.

CONCLUSIONES

La seguridad de la información no sólo debe entenderse como un conjunto de elementos técnicos y físicos, sino como un proceso cultural de personas y organizaciones. Si el usuario es el eslabón más débil, deben existir controles que ayuden a disminuir el riesgo que éste pueda representar.

Kevin Mitnick, el hacker más reconocido a nivel mundial y experto en Ingeniería Social, concluye: “Puedes gastar una fortuna en tecnología y servicios… y como sea, tu infraestructura de red podría estar vulnerable a la forma más vieja de manipulación”.

Ahora que conoces más sobre la ingeniería social y la seguridad de la información, la próxima vez que sientas que tu información está completamente segura, recuerda que no todas las intrusiones son siempre tan obvias como esta:

Img. 5 Cortesía Flickr

Referencias

- GRANGER, Sarah; **Social Engineering Fudamentals, Part I: Hacker Tactics**;
- HEARY, Jamey; **Top 5 Social Engineering Exploit Techniques**;
- DOLAN, Aaron; **Social Engineering**; http://www.sans.org/reading_room/whitepapers/engineering/social-engineering_1365
- RAMÍREZ, Jorge; **Ingeniería Social, una amenaza informática** http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica
- **The Official Social Engineering Portal**

[1] MOLIST, Mercè; Ingeniería Social: Mentiras en la Red; http://ww2.grn.es/merce/2002/is.html