ESTUDIO DETALLADO DE LA INGENIERIA SOCIAL

@FrankStark

Introducción

Este documento está destinado a proporcionar una explicación detallada de la Ingeniería Social, además de describirnos en qué consiste. También cubre un estudio de caso con el fin de ofrecer una mejor comprensión de cómo la ingeniería social juega un papel importante en los ataques que se llevan a cabo en vida real.

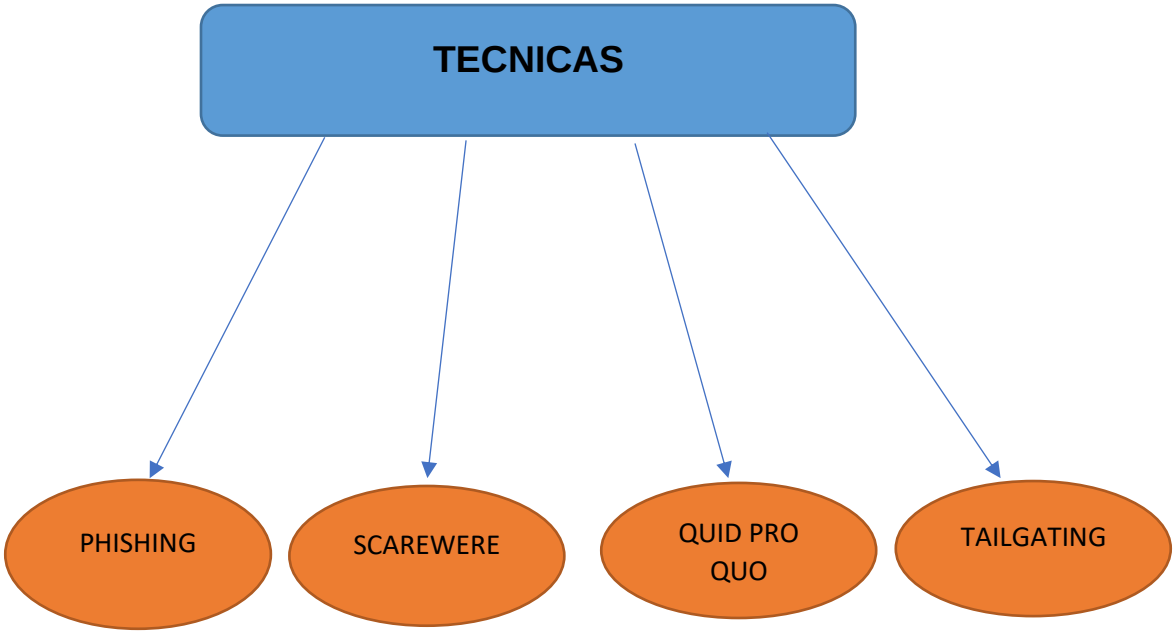
Palabras clave

Vishing, Phishing, Smishing, Impersonation, Pretexting, Water Holing, Baiting, Tailgating, Quid Pro Quo

Definiciones

INGENIERIA SOCIAL. - En el contexto de la Ciberseguridad, la ingeniería social es la técnica de manipulación que explota el error humano para obtener información privada o acceso a ella. En el ciberdelito, estas estafas de "piratería humana" tienden a atraer usuarios desprevenidos para que expongan datos, propaguen infecciones de malware o acceso a sistemas restringidos.

Estas son algunas técnicas populares de ingeniería social utilizadas por atacantes y grupos de APT para obtener información y datos confidenciales.



Vishing. – Este es también conocido como "Phishing de Voz", definido como un método de Ingeniería Social a través de la comunicación telefónica para obtener acceso a información personal, privada o información financiera del objetivo, con el fin de obtener una recompensa económica. También es utilizado para recolectar información del contexto donde se realizará el ataque.

Phishing. - Es un método de Ingeniería Social en donde el atacante obtiene información privada haciéndose pasar por una entidad/institución confiable y se entabla una comunicación principalmente a través de correos electrónicos. El correo electrónico generalmente contiene un vínculo a una página web fraudulenta que parece legítima, con logotipos, contenido y formularios para depositar la información que se pretense sustraer, como por ejemplo cuentas bancarias o información de las tarjetas de crédito.

Smishing. - Es una técnica de Ingeniería Social que implica el uso de SMS para atraer a las víctimas a un curso de acción específico, es la práctica del phishing mediante SMS.

Suplantación. – Es una técnica de ingeniería social que consiste en fingir ser otra persona con el motivo de acceder a un área específica, edificio, o incluso un dispositivo.

Pretexting.- Es el acto de crear un escenario falso para involucrar a un víctima objetivo de tal manera que las posibilidades de que la víctima objetivo proporcione información o llegue a realizar acciones que ayuden al atacante a obtener acceso a su sistema.

Water holing.- Es una estrategia de ingeniería social dirigida, basada en la confianza que los usuarios tienen en los sitios web que visitan con regularidad. El atacante aprovecha la confianza de una víctima en un sitio web e infecta el sitio web con malware que se utilizará además para obtener acceso y / o información del dispositivo de la víctima.

El Cebo. - Es la práctica de la Ingeniería Social de atraer a las víctimas trabajando en la naturaleza inherente de la codicia y la curiosidad. Un atacante deja un malware infectado, por ejemplo, una unidad USB (llamada Rubber Ducky) en un punto de acceso y espera a que la víctima caiga en la trampa, tomando la USB y usandola. Una vez que la víctima lo levanta y lo enchufa en su dispositivo personal o corporativo, su dispositivo se infectará con el malware y el atacante tendrá acceso a toda la información personal que necesite.

Tailgating.- Es la técnica de ingeniería social de buscar la entrada a un área restringida o edificio simplemente caminando detrás de una persona que tiene acceso a esa ubicación en particular.

Quid Pro Quo.- Es un ataque de ingeniería social en donde el atacante solicita el intercambio de datos críticos o credenciales de inicio de sesión a cambio de un servicio (a menudo disfrazado de soporte técnico).

Vectores para la ingeniería social

1. Vishing
2. Phishing
3. Smishing
4. Suplantación

Claves Principales

Hay 6 principios clave de cualquier ataque de ingeniería social, estos se establecieron por Robert Cialdini.

6 leyes que amenazan los elementos humanos de la seguridad

Peculiaridades del cerebro

- Reciprocidad
- Consistencia
- Aceptación social
- Escasez
- Autoridad
- Gusto

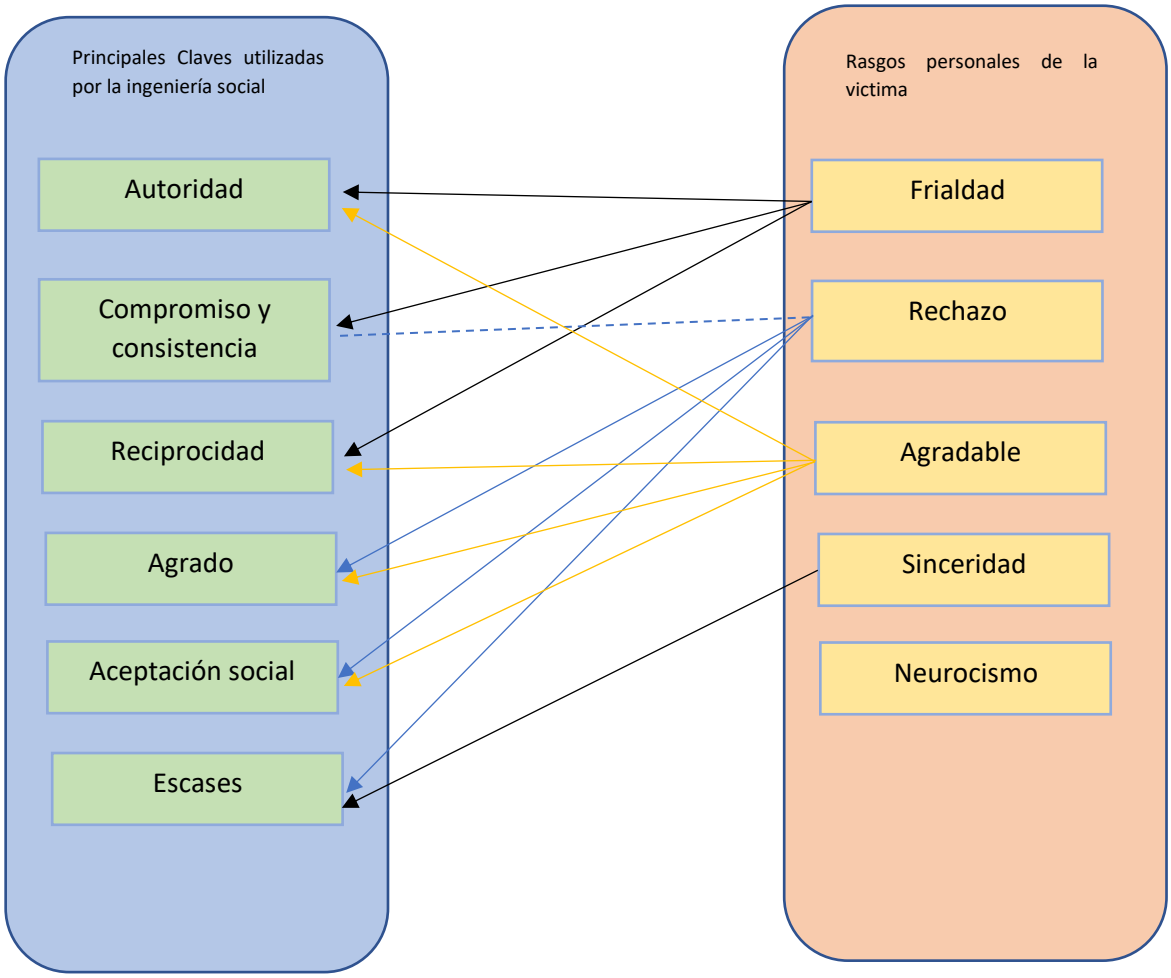
Reciprocidad.- Esta se basa en que la gente tiene la naturaleza de devolver cualquier favor que alguien haya prestado. La gente corresponde a los hechos y actos realizados hacia ellos. La estrategia de la policía se basa en este principio.

Compromiso.- Si las personas se comprometen con algo, oralmente o por escrito, es más probable que cumpla lo prometido y se apegue a su acuerdo, ya que representa su propia imagen y compromiso.

Aceptación social.- Se basa en que la gente hará las cosas que otras personas hacen, por lo mismo necesitan para encajar en la sociedad y ser aceptadas. También encontramos AUTORIDAD: las personas tienen una naturaleza inherente para responder al liderazgo, por lo que tenderá a obedecer a figuras autorizadas incluso si se les pide que realicen
actos objetables.

Agrado.- Las personas son fácilmente manipuladas e influenciadas por otras personas que ellos admiran o les gusta.

Escasez.- Notar la escasez generará demanda entre las personas.



Case de estudio sobre Ingeniería Social

(El Caso de la "PIZZA")

Los piratas informáticos se hicieron pasar por un servicio de entrega de pizzas y con ello llevaron a cabo la aplicación de ingeniería social de una forma muy exitosa, el ataque a la sucursal de Varsovia perteneciente a una conocida empresa internacional, en donde por cuestión de minutos infectaron el sistema de TI mediante la implementación de malware.

Todo comenzó cuando empezaron a sustraer la información a las direcciones de correo electrónico de los empleados de las empresas que figuran en los sitios web.

La información que se envió a todos los correos electrónicos de los empleados fue relacionada con el lanzamiento de la venta de una nueva pizza y que habría un descuento del 30% para los primeros clientes, también que esta promoción estaba limitada a solo unos cuantos.

Los empleados tentados por esta oferta comenzaron a realizar pedidos llegando a realizar pedidos de hasta 8 cajas de pizza. Después de algún tiempo apareció el repartidor de pizzas con las 8 cajas de pizza y un regalo en forma de lámparas LED conectadas por USB que cambiaban de color al ritmo de la música. Sorprendidos con el regalo, los empleados conectaron el USB a sus computadoras.

No sabían que de esta manera les daban a los hackers acceso remoto a la infraestructura de la empresa y con una computadora los piratas informáticos pudieron comprometer toda la red.

Contramedidas

1. Los empleados deben estar capacitados en varios protocolos y técnicas de seguridad.

2. Los mensajes que soliciten detalles de seguridad deben eliminarse e informarse, es probable que estos mensajes sean fraudulentos.

3. Deben implementarse filtros de spam para el correo electrónico.

4. Solo se debe acceder a sitios web seguros.

5. El software antivirus debe actualizarse periódicamente.

6. Deben realizarse pruebas periódicas sin previo aviso de los marcos de seguridad.

Referencias

- https://en.m.wikipedia.org/wiki/Social_engineering_(security)
- https://www.itsecurityawareness.ie/a-z-glossary-of-information-security-and-social-engineering-terms