
9. Ingeniería Social
Julio Javier Iglesias Pérez
C|EH Julio Iglesias Pérez

¿Qué es la Ingeniería Social?

Es el arte de convencer a la gente de revelar información confidencial.

Comportamientos vulnerables a los ataques

- Naturaleza humada a la confianza.
- Ignorancia sobre la ingeniería social.
- Obligación moral.
- Etc.

Factores que hacen a las compañías vulnerables

- Entrenamiento sobre seguridad insuficiente.
- Fugas de políticas de seguridad.
- Fácil acceso a la información.
- Muchas Unidades organizativas

- La Ingeniería social es efectiva porque los errores humanos son más susceptibles.
- Es difícil detectar intentos de ingeniería social.
- No hay métodos para asegurarse completamente contra ataques de ingeniería social.
- No hay ningún software o hardware que defienda contra la ingeniería social.

Típicas señales de Ingeniería social

- Mostrar rápida a inadvertidamente el nombre.
- Utilizan elogios.
- Muestra disconformidad cuando es cuestionado.
- Pretende, reclama autoridad si la información no es provista.
- Hacen solicitudes informales.
- Etc.

Fases de un ataque de ingeniería social

- Research: Dumpster diving (buceo de basurero), sitios web, empleados, etc. Crean relaciones con empleados selectos.
- Develop: Eligen al empleado víctima.
- Exploit: Seleccionan a la víctima, identifican empleados frustrados, etc. Explotan la relación, recolectan información sensible, información financiera, tecnologías que utilizan en su compañía, etc.

Impactos en la organización

- Pierde privacidad.
- Peligros de terrorismo.
- Pérdidas económicas.
- Daño, etc.

Ataques de inyección de comandos

- Online: Internet, acercarse a los empleados, persuadir.
- Teléfono: Imitación de un usuario legítimo.
- Acercamiento personal. Obtener información preguntando directamente.

Blancos comunes de Ingeniería Social

- Relaciones y Help Desk.
- Usuarios y clientes.
- Vendedores de la organización.
- Administradores de sistemas.
- Soporte técnico.
- Hacerse pasar por trabajadores de la organización.

Tipos de Ingeniería Social

Human-based. Obtienen información sensible por interacción, miedo, confianza y la naturaleza humana de ayudar.

- Fingiendo ser un usuario legítimo, dar la identidad y preguntar por información sensible. "Hola soy Juan de departamento de Ventas...."
- Fingiendo ser un usuario importante, haciéndose pasar por ejemplo con un cliente importante.
- Fingiendo ser de soporte técnico. "Don Juan, aquí habla xx de soporte, ayer tuvimos un problema con el sistema, y estamos revisando si está todo OK, me puede dar su nombre de usuario?"

Tipos de Ingeniería Social

- Eavesdropping: Escucha de conversaciones no autorizada, o lectura de mensajes, intercepción de audio, video, etc.
- Shoulder Surfing: Procedimiento de robar passwords, identificación personal, números de cuentas, etc. Viendo sobre su hombro (shoulder) a la distancia tratando de obtener dicha información.

Tipos de Ingeniería Social

- Dumpster Diving: Buscar un "tesoro" en la basura de alguien. Información de contacto, pagos de teléfono, información de operaciones, información financiera, etc.
- Tailgating: Una persona no autorizada con una maleta entra a un área segura siguiendo a una persona autorizada cerca de una puerta con acceso con llaves o sensores, etc.

Tipos de Ingeniería Social

- In person: Recolectar información sobre tecnologías que utilizan, información de contactos, etc.

- Third-Party Autorization: Referirse a una persona importante de la organización y tratar de recolectar datos. "Don Pepe, nuestro jefe administrativo me pidió que lleve los reportes de auditoría"


ORIGINAL MOTION PICTURE SOUNDTRACK
MATCHSTICK MEN
C|EH Julio Iglesias Pérez
MUSIC BY
HANS ZIMMER


TO SOLVE THE HARDEST CRIMES, HIRE THE SMARTEST CRIMINAL.
WHITE COLLAR
NEW ORIGINAL SERIES
FRIDAYS 10/9C
usa
C|EH Julio Iglesias Pérez

Tipos de Ingeniería Social

- Computer-based. Utilizando la ayuda de computadoras.
- Pop-ups preguntando por información personal, GANASTE 1 millón de dólares.
- Mails o cartas engañosas (Hoax) indicando que están infectado con virus, troyanos, worms, etc.
- Cadenas de correos ofreciendo regalos gratis, etc.
- Por mensajería obteniendo información personal.
- Correo spam irrelevante, no deseado, no solicitado para recolectar información financiera, números de identificación, información de la red, etc.
- Phishing páginas web falsas, bancos, ebay, etc.
- Utilizando SMS, pidiendo tarjetas de crédito, información sensible.

Tipos de Ingeniería Social

Insider attack

- Espiando: Especialmente los competidores.
- Venganza: Personas enojadas, empleados enojados o frustrados.
- 60% de los ataques ocurren detrás del firewall. Un ataque interno es fácil de realizar. La prevención es difícil.

Prevención de amenazas internas

No existe una prevención fácil para las amenazas internas.

- Políticas legales.
- Auditorías y logging.
- Acceso controlado.
- Privilegios mínimos.
- Reparación y rotación de deberes.
- Archivar datos críticos.

Prevención de amenazas internas

Ingeniería Social en las redes sociales para obtener información personal y/o sensible de los usuarios.

Riesgos de la ingeniería social en la red de las organizaciones

- Robo de datos, riesgo de explotación de información.
- Fuga involuntaria de información, sin saberlo muestra, postea o publica información sensible de la organización.
- Ataques dirigidos, reconocimiento preliminar.
- Vulnerabilidad de la red, fallas o bugs en la red.

Riesgos de la ingeniería social en la red de las organizaciones

Robo de identidad

- Robo de información personal, ocurre cuando una persona roba su nombre y/u otra información personal para propósitos fraudulentos.
- Pérdida de números de seguridad social, el impostor obtiene información personal, como números de licencias, de identificación, etc.

Ejemplo

- Paso 1. Obtener información de pagos de agua, electricidad, dumpster diving, stolen mail u onsite stealing.
- Paso 2. Ir al departamento de vehículos y decirles que perdiste tu licencia de conducir. Ellos van a intentar probar tu identidad como por ejemplo pedirte pagos de luz, agua, etc. Se les muestra los bills robados, que te has movido de la dirección original. Se llenan dos formularios, se necesitará una foto para la licencia, se remplaza la foto de la licencia y listo :)

Ejemplo

- Paso 3. Ir al banco con la cuenta original del que se robó y decirles que necesitan una nueva tarjeta de crédito. Decirles que no recuerdas el número de cuenta. Luego les muestras la licencia trucha. Listo para hacer compras.

Contramedidas

Políticas

1. Password Policies: Periódicamente cambiar las contraseñas. Impedir el uso de contraseñas fáciles de adivinar. Bloquear cuenta luego de intentos fallidos. Longitud y complejidad de contraseñas. Mantener en secreto las contraseñas, no escribirlas RECORDARLAS

Contramedidas

2. Physical Security Policies: Identificación de empleados utilizando tarjetas de identificación, uniformes, etc. Escoltar a los visitantes. Áreas restringidas. Triturar información apropiadamente de documentos que ya no sirven. Emplear personal de seguridad.

Otras contramedidas

- Un programa de entrenamiento eficiente que debe consistir en todas las políticas y métodos de seguridad para incrementar la conciencia de la Ingeniería Social.
- Guías Operativas para asegurar la seguridad de la información sensible del uso no autorizado de los recursos.

También

- Clasificación de la información: Categorizar la información como top secret, propietario, para uso interno solamente, para uso público, etc.
- Privilegios de acceso: Debe haber un administrador, usuario, cuentas de invitados con autorización apropiada.
- Revisión de empleados y terminación de procesos apropiada.
- Tiempo de respuesta a incidentes apropiado: Debe haber una guía para la reacción en caso de un intento de ingeniería social.

También

Two factor authentication: El uso de dos factores incrementará notablemente la seguridad. Hay tres tipos de autenticación:

1. Algo que sé, como una contraseña.
2. Algo que tengo, como una tarjeta inteligente.
3. Algo que soy, biométrico.

¿Cómo detectar correos Phishing?

Ver bien la dirección, ver que se use SSL, los bancos no piden información de ese tipo por correo.

Anti-Phishing Toolbar: Netcraft, PhishTank. Ayudan a detectar sitios Phishing.

Contramedidas para el robo de identidad

- Asegurar o triturar los documentos conteniendo información privada.
- Para mantener tu correo seguro, vaciar el mailbox rápidamente.
- Asegurarte que tu nombre no esté presente en la lista marketers' hit.
- Sospechar y verificar todas las solicitudes de datos personales.
- Revisar los reportes de tarjeta de crédito regularmente.

Contramedidas para el robo de identidad

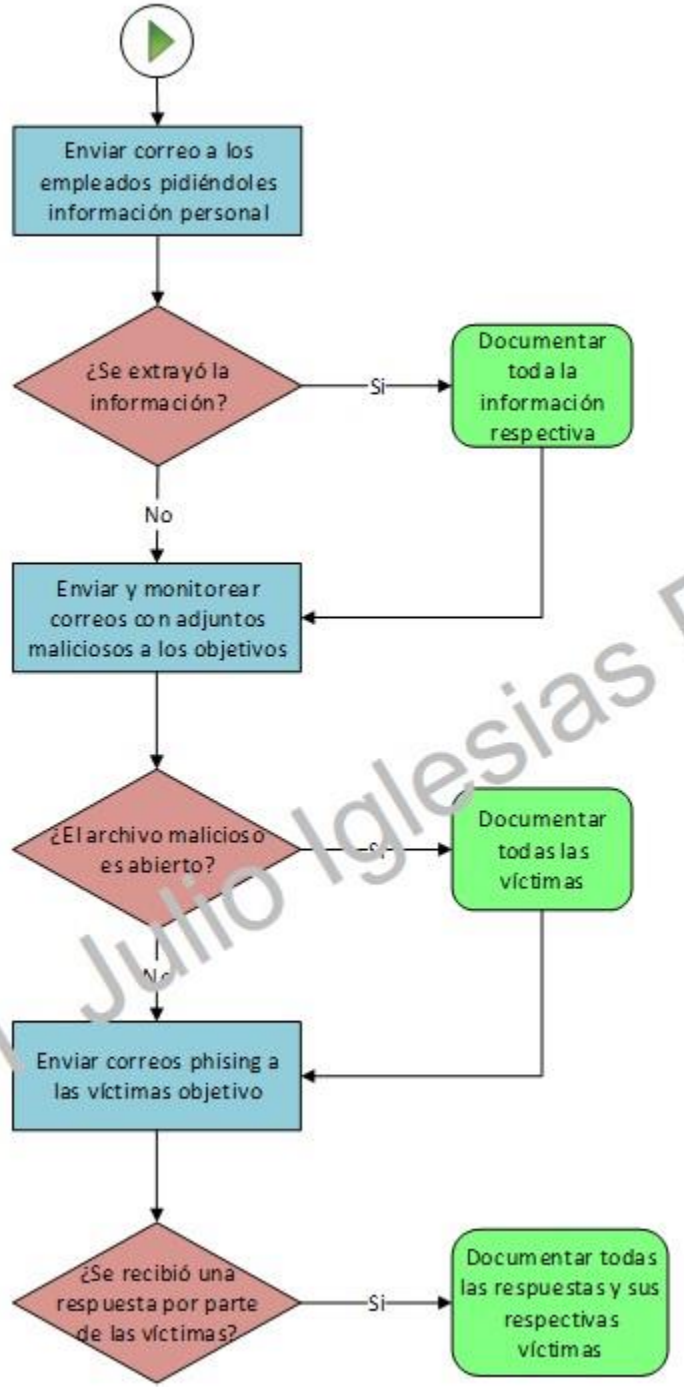
- Nunca dejar tu tarjeta fuera de tu vista.
- Proteger tu información personal que sea publicada.
- Nunca dar información personal por teléfono.
- No mostrar números de cuenta o contactos a menos que sea obligatoria.

Pentesting de Ingeniería Social

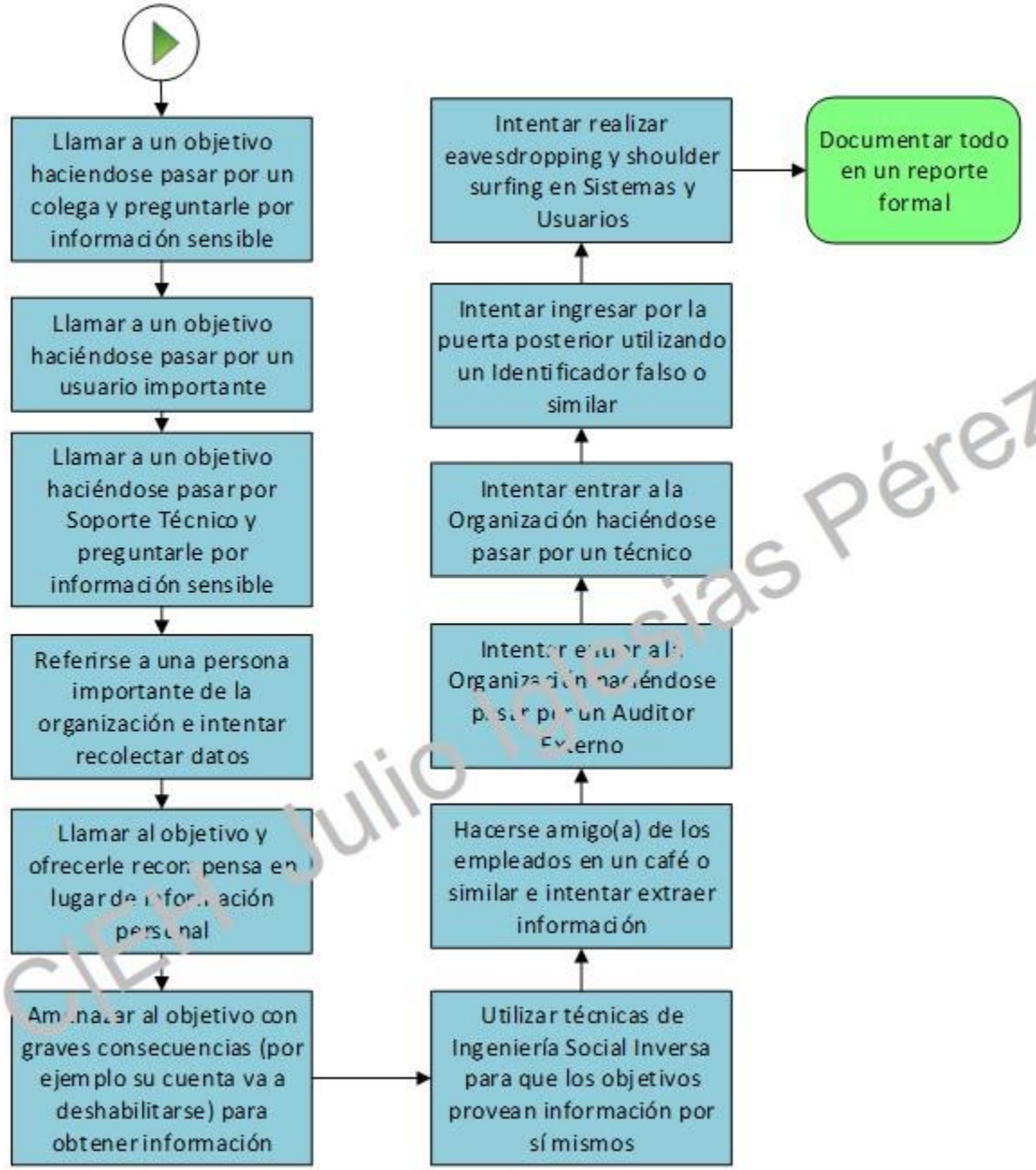
El objetivo es hacer un pen test a los factores de fortaleza humanos.

Ser extremadamente cuidadosos y profesionales.


Pentesting de Ingeniería Social: Utilizando E-Mail
C|EH Julio Iglesias Pérez




Pentesting de Ingeniería Social: Utilizando Teléfono
C|EH
Julio Iglesias Pérez




¡Muchas Gracias!
C|EH Julio Iglesias Perez