Ingeniería social

"El engaño como arma del delito"

Por: Amairanis Saldaña

¿Qué es la Ingeniería Social?

Concepto General

Es tomado de las Ciencias Sociales, como aquella práctica que implica el uso de **la manipulación con el fin de conseguir un objetivo.**

Como Trabajan

La ingeniería social se ejecuta con el fin de **engañar a víctimas inocentes** para que compartan sus datos personales.

Tecnica mas usual

Los ciberdelincuentes que se basan en la **generación de confianza** por medio del lenguaje amable, empático o atractivo.

Formas en que lo hacen

Se pueden llevar a cabo **fuera de la red**, por una **llamada telefónica** o, incluso, con la visita inesperada de una persona a una oficina solicitando determinada información de la empresa.

Tácticas que Utilizan

Suplantando la identidad de una marca de confianza

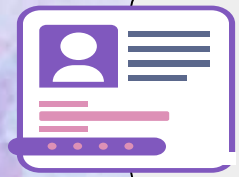
Hacerse pasar por una agencia gubernamental o una figura de autoridad

Inducir miedo o sensación de urgencia

Apelar a la codicia

Apelar a la amabilidad o la curiosidad

Consecuencias

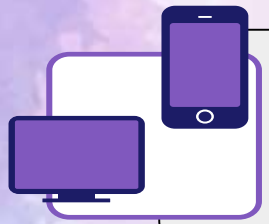


Pérdida financiera:

Robo de identidad, fraudes, y pérdidas económicas significativas.

Pérdida de datos confidenciales:

Exposición de información sensible, como secretos comerciales o datos de clientes.



Daño reputacional:

Compromiso de la imagen de una empresa o institución.

Interrupción de los servicios:

Ataques a infraestructuras críticas pueden causar interrupciones en servicios esenciales.

Amenazas de la Ingenieria Social

Phishing

Tailgating

Scareware

Baiting

Pretextar

Ataque de abrevadero

Phishing


¿CÓMO FUNCIONA EL PHISHING?
¿QUÉ TIPO DE INFORMACIÓN ROBA?
DATOS PERSONALES
Direcciones de correo
Número de documento de identidad
Datos de localización y contacto
INFORMACIÓN FINANCIERA
Número de tarjetas de crédito
Números de cuentas
Información de Home Banking o e-commerce
CREDENCIALES DE ACCESO
Redes Sociales
Cuentas de correo
PRINCIPALES MEDIOS DE PROPAGACIÓN
CORREO ELECTRÓNICO
REDES SOCIALES
SMS/MMS
LLAMADAS TELEFÓNICAS
INFECCIÓN DE MALWARE
#SECURITIP
#CONSEJOSALVADOR

Tipos de Fraude Phishing

Los correos electrónicos masivos de phishing se envían a millones de destinatarios a la vez. Parecen ser enviados por una empresa u organización grande y conocida, como un banco nacional o mundial, un gran minorista en línea, un popular proveedor de pagos en línea, etc., y hacen una petición genérica como «*tenemos problemas para procesar su compra, actualice su información de crédito*».

El spear phishing tiene como objetivo una persona concreta, normalmente alguien con acceso privilegiado a la información de los usuarios, a la red informática o a los fondos de la empresa. Un estafador investigará al objetivo, a menudo utilizando información que se encuentra en LinkedIn, Facebook u otras redes sociales para crear un mensaje que parezca proceder de alguien que el objetivo conoce y en quien confía o que haga referencia a situaciones con las que el objetivo está familiarizado.

El whale phishing es un ataque de suplantación de identidad rápida que se dirige a una persona de alto perfil, como un director general o un conocido cargo político. En un correo corporativo comprometido (BEC), el hacker utiliza credenciales comprometidas para enviar mensajes de correo electrónico desde la cuenta de correo electrónico real de una figura de autoridad, lo que hace que la estafa sea mucho más difícil de detectar.

Según el IBM Security X-Force Threat Intelligence Index de 2023, **el phishing es el principal vector** de infección de malware, identificado en el 41 % de todos los incidentes. Según el informe "Coste de una filtración de datos" de 2024, el phishing es el vector de ataque inicial que conduce a las vulneraciones de datos más costosas.

Baiting

Mediante un señuelo se atrae (sin doble sentido) a las víctimas para que, consciente o inconscientemente, faciliten información confidencial o descarguen código malicioso, tentándolas con una oferta valiosa o incluso un objeto de valor. Aunque algunas estratagemas utilizadas como señuelo no son nada elaboradas. **Por ejemplo**, algunos actores de amenazas dejan unidades USB infectadas con malware donde la gente las encuentra, cogen y utilizan porque «oye, un USB gratis».

En el tailgating, también llamado **«piggybacking»**, una persona no autorizada sigue de cerca a una persona autorizada hasta una zona que contiene información sensible o activos valiosos. El seguimiento puede realizarse en persona, por ejemplo, un actor de amenazas puede seguir a un empleado a través de una puerta desbloqueada.

En el pretexto, el actor de la amenaza crea una situación falsa para la víctima y se hace pasar por la persona adecuada para resolverla. Con frecuencia (y lo que es más irónico), el estafador afirma que la víctima se ha visto afectada por una violación de seguridad y, a continuación, se ofrece a realizar las correcciones, para lo cual la víctima le proporcionará información importante sobre su cuenta o el control de su ordenador o dispositivo. Técnicamente hablando, casi todos los ataques de ingeniería social implican algún grado de pretexto.

También considerado una forma de malware, el scareware es un software que utiliza el miedo para manipular a las personas para que compartan información confidencial o descarguen malware. El scareware suele adoptar la forma de un falso aviso de las fuerzas de seguridad acusando al usuario de un delito, o de un falso mensaje de soporte técnico advirtiéndole de la presencia de malware en su dispositivo.

Prevenciones contra La Ingenieria Social

Formación de concienciación sobre seguridad

Políticas de control de acceso

Tecnologías de ciberseguridad

Verificación de la identidad

Ventajas y Desventajas

Ventajas

- Si bien la ingeniería social se utiliza principalmente con fines maliciosos, también puede tener aplicaciones legítimas, como en las pruebas de penetración para evaluar la seguridad de un sistema. Sin embargo, es esencial que estas pruebas se realicen con autorización y siguiendo las mejores prácticas éticas.

Desventajas

- Las desventajas de la ingeniería social incluyen el robo de información sensible, pérdida de confianza y reputación, altos costos de recuperación, impacto negativo en la moral de los empleados, dificultad para prevenir ataques debido a su naturaleza psicológica, y posibles consecuencias legales. La creciente digitalización aumenta la vulnerabilidad, por lo que es crucial implementar capacitación en seguridad para mitigar estos riesgos.

Ejemplo

1. El virus ILOVEYOU (2000)

En el año 2000, surgió un insidioso gusano informático conocido como el virus ILOVEYOU, que provocó una crisis mundial en la seguridad digital. Era el 5 de mayo cuando este aparentemente inocente archivo adjunto a un correo electrónico comenzó su andadura, disfrazado de carta de amor.

El impacto fue inmediato y asombroso: **más de diez millones de** ordenadores personales con Windows fueron infectados, según informó Wired.

Este virus no sólo explotaba las vulnerabilidades del software, sino que también jugaba con la curiosidad y el deseo de conexión naturales del ser humano. Fue un duro recordatorio de cómo un simple clic puede provocar un caos generalizado en el ámbito digital.

Videos Instruccional sobre La Ingenieria Social

Recomendaciones

01

Capacitar regularmente a empleados y usuarios sobre los riesgos de la ingeniería social.

02

Aplicar políticas de doble autenticación para asegurar los accesos a cuentas sensibles.

03

Mantener sistemas actualizados y con las configuraciones de seguridad óptimas.

04

Establecer canales de verificación: Nunca confiar ciegamente en solicitudes de información y verificar siempre la identidad de quienes las hacen.

Conclusiones

La ingeniería social es una amenaza constante para la seguridad de la información. La mejor defensa es una combinación de tecnología y concientización humana. Al comprender las tácticas de los atacantes y adoptando medidas preventivas, podemos protegernos de los riesgos de la ingeniería social.