Áreas Transversales: Sociales, Castellano, matemáticas, artística, sociales, economía, inglés.

Elabora: Gigliola Martínez

TIEMPO: 1 ___ 2 X

COMPETENCIAS: Orientación al resultado, cognitivo

PROPÓSITO: Conocer acerca de la ingeniería social

INDICADORES DE DESEMPEÑO:

Utilización de la ofimática para procesar información y recolección de datos de la idea de negocio.

TEMA: ingeniería social

METODOLOGÍA INSTITUCIONAL C3

CONCIENTIZACIÓN

Vídeo: ingeniería social

CONCEPTUALIZACIÓN

Lea el texto:

INGENIERÍA SOCIAL

La ingeniería social es el arte de manipular a las personas para que divulguen información confidencial o realicen acciones que pueden comprometer su seguridad. Este tipo de ataque se basa en la construcción de confianza o la explotación de emociones humanas como el miedo, la urgencia o la curiosidad para engañar a las víctimas y hacer que revelen datos sensibles, como contraseñas, información bancaria, o acceso a sistemas protegidos.

Según Kevin Mitnick, existen **4 principios básicos en la Ingeniería Social** que son comunes a todas las personas (o en su gran mayoría:

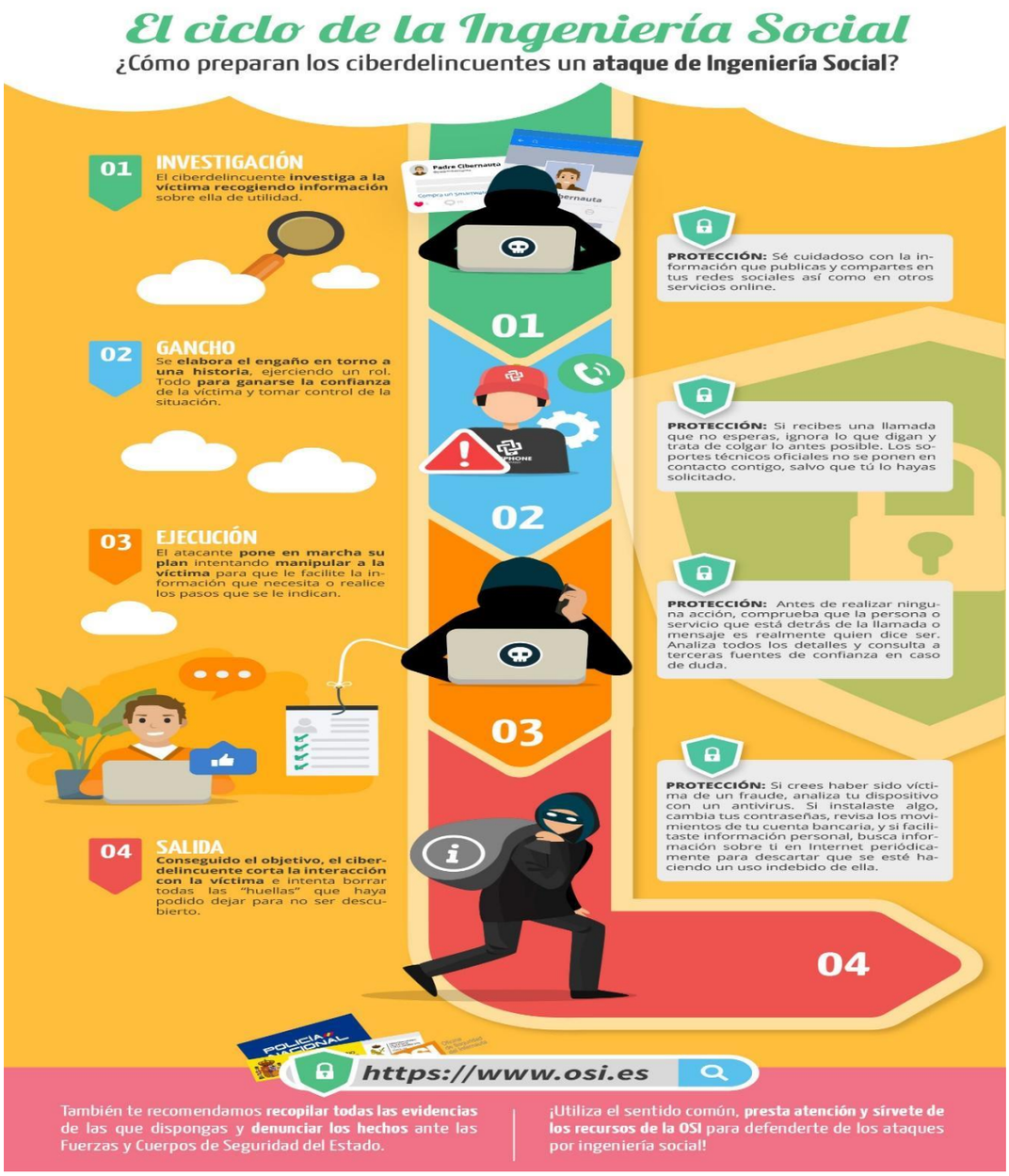
- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir No.
- A todos nos gusta que nos alaben.

Otros factores que se presentan:

En sistemas de información o en redes, el eslabón más débil de la cadena siempre es el usuario.

El miedo y la codicia.

La inocencia y la credulidad



Por lo general, los atacantes que usan la ingeniería social tienen dos objetivos:

1. Sabotaje: alterar o corromper los datos para causar daños o molestias.
2. Robo: obtener objetos de valor como información, acceso a sistemas o dinero.

¿Quiénes Hacen Ingeniería Social?

Detectives privados. Miembros de organismos policiales y/o de inteligencia gubernamental o comercial.

Delincuentes organizados.

Hackers y Crackers (delincuentes organizados, pero orientados hacia la Tecnología de Información).

Personas curiosas que sientan el deseo de obtener información acerca de otras personas

TIPOS DE ATAQUES DE INGENIERIA SOCIAL

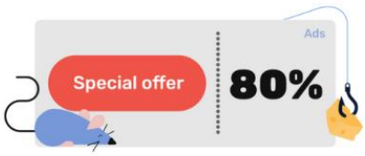
Scareware

Hackeo de correos electrónicos y spam de contactos

Acceso a seguimiento de personas

Phishing

Suplantación de DNS



Baiting

Infracciones físicas

Pretextar

Ataques de pozo de agua

Quid pro quo

Elaborado por: Arleth

1. Scareware

El scareware es malware que tiene como objetivo asustarlo para que tome medidas, y tome medidas rápidamente. A menudo se presenta en forma de ventanas emergentes o correos electrónicos que indican que debe actuar ahora para deshacerse de virus o malware en su dispositivo.

2. Hackeo de correos electrónicos y spam de contactos

Los ingenieros sociales lo saben muy bien, requisando cuentas de correo electrónico y enviando spam a las listas de contactos con estafas y mensajes de phishing.

3. Acceso a seguimiento de personas

El seguimiento de acceso es cuando un ingeniero social rastrea o sigue físicamente a una persona autorizada a un área a la que no tiene acceso. Una vez dentro, tienen pleno dominio para acceder a los dispositivos que contienen información importante.

4. Phishing

El phishing es una forma bien conocida de obtener información de una víctima involuntaria. Funciona normalmente, cuandoun ciberdelincuente envía un mensaje a un objetivo que solicita algún tipo de información o acción que podría ayudar con un delito más importante.

5. Suplantación de DNS

También conocida como envenenamiento de caché, la suplantación de DNS es cuando se manipula un navegador para que los usuarios en línea sean redirigidos a sitios web maliciosos empeñados en robar información confidencial.

6. Baiting (Cebo)

El cebo se basa en la premisa de que alguien muerde el anzuelo, lo que significa colgar algo deseable frente a la víctima y esperar que muerda. Esto ocurre con mayor frecuencia en sitios peer to peer como las redes sociales.

7. Infracciones físicas

Como su nombre lo indica, las infracciones físicas ocurren cuando un ciberdelincuente está a la vista, haciéndose pasar físicamente por una fuente legítima para robarle datos o información confidencial.

8. Pretextar

Es cuando un ingeniero social hace uso de un pretexto interesante para captar la atención de alguien. El ingeniero social intenta engañar a la posible víctima para que proporcione algo de valor, en donde a menudo el ingeniero social se hace pasar por una fuente legítima.

9. Ataques de pozo de agua

Un ataque de pozo de agua es un ataque de un solo barrido que infecta una sola página web con malware. La página web casi siempre se encuentra en un sitio muy popular, o en un abrevadero virtual, por así decirlo, para garantizar que el malware pueda llegar a tantas víctimas como sea posible.

10. Quid pro quo (un favor por un favor)

En el caso de la ingeniería social, la víctima arroja información confidencial, como inicios de sesión de cuentas o métodos de pago, y luego el ingeniero social no devuelve su parte del trato.

Cómo Evitar La Ingeniería Social

Una vez que cae en las redes de un ingeniero social, puede ser difícil librarse de ellas. La mejor manera de evitar los ataques de ingeniería social es saber cómo detectarlos. Afortunadamente, no necesita ser un experto en tecnología para seguir buenas prácticas de ingeniería social. Lo único que necesita es su intuición y sentido común.

Instale software antivirus de confianza
Puede ahorrarse el tiempo y las molestias de tener que comprobar las fuentes gracias a software antivirus de confianza capaz de detectar mensajes o páginas web sospechosos.

Cambie la configuración de spam en el correo electrónico
También puede ajustar su configuración del correo electrónico para fortalecer los filtros de spam si estos mensajes aparecen en su bandeja de entrada. Dependiendo del cliente de correo electrónico que utilice, el procedimiento podría ser ligeramente distinto, así que lea nuestra guía para evitar spam en el correo electrónico.

Investigue la fuente
Si recibe un mensaje de correo electrónico, un SMS o una llamada telefónica de una fuente no conocida, busque esa dirección o ese número de teléfono en un motor de búsqueda para ver qué aparece. Si forma parte de un ataque de ingeniería social, el número o la dirección de correo electrónico puede haberse identificado como tal previamente. Incluso si el remitente parece legítimo y así lo intenta asegurar, compruébelo de todos modos, porque la dirección de correo electrónico o el número de teléfono podrían ser ligeramente diferentes a los de la fuente real, y podrían estar vinculados a una página web no segura.

Si algo parece demasiado bueno para ser cierto, seguramente sea falso
Parece bastante claro que famosos regalando miles de dólares en bitcoines suena demasiado bueno para ser verdad. En este tipo de ataque de ingeniería social, la intención y sentido común pueden ser muy útiles. No se fíe de ofertas que prometen grandes recompensas a cambio de algo de dinero o información. Y, si la solicitud parece venir de alguien que conoce, pregúntese «¿De verdad me pediría esta información de este modo? ¿De verdad compartiría este enlace conmigo?».

6 Principios De La Ingeniería Social

La Ingeniería Social tiene algunos elementos básicos con los que un atacante juega para ganarse la confianza suficiente y engañar a la víctima.
Según Pablo F. Iglesias, consultor especializado en materia digital y ciberseguridad, existen 6 principios de la Ingeniería Social similares a los principios básicos de las ventas de Cialdini:

- RECIPROCIDAD: Cuando una persona nos ofrece algo, por lo general, solemos tender a ofrecerle también algo. Por el contrario, si esa persona no nos trata con respeto,

estaremos más susceptibles a pagarle con la misma moneda. Así pues, la reciprocidad es un «instinto» social fácilmente manipulable.

- URGENCIA: La mayoría de los ataques de Ingeniería Social consiguen que las personas piquen a través de la urgencia. Ejemplos: "¡Alguien ha accedido a tu cuenta bancaria, entra en el siguiente enlace para solucionarlo y proteger tu dinero!", "¡Esta oferta sólo durará durante los próximos cinco minutos!" o "Tu ordenador ha sido infectado, haz clic aquí para borrar el virus ahora".

- CONSISTENCIA: Si, en algún momento, hemos dado nuestra palabra, tendemos más a cumplir con ello que a no hacerlo. Un ejemplo de ataque de Ingeniería Social utilizando este principio es, por ejemplo, cuando un trabajador de una empresa pide a la víctima que realice determinadas tareas habituales. Empezando por pequeñas acciones y continuando por otras más delicadas. A pesar de que una de esas tareas pueda parecer rara, al haberse comprometido, la llevará a cabo junto al resto. De esta manera, el ingeniero social consigue manipular por consistencia.

- CONFIANZA: Nuestra desconfianza se reduce cuando el interlocutor con el que hablamos nos cae bien o está alineado con nuestros intereses o valores. Un ejemplo de ello lo podemos observar cuando los altos directivos o trabajadores con acceso a contenido o servicios confidenciales (gobierno, corporaciones, policías, militares…) son «seducidos» por perfiles que se ganan su confianza lo suficiente como para que tengan un descuido y puedan aprovecharse de él. A continuación, es cuando el ingeniero social los extorsiona si no cumplen sus exigencias. Cuando se da una componente sexual o amorosa se denomina sextorsion.

- AUTORIDAD: Cuando una persona en prácticas de una empresa pide las credenciales de acceso de un servicio, lo más probable es que sea vista con desconfianza. No obstante, si las mismas credenciales son pedidas por un Director/a, la situación cambia. De esta manera, la usurpación de identidad juega un papel clave, ya sea de forma real (robo del perfil digital del Director/a) o ficticia (clonado de perfiles o phishing).

- VALIDACIÓN SOCIAL: Si recibimos un correo electrónico en el que se nos pide hacer una determinada acción, la cual es extraña, lo más seguro es que nos pensemos si llevarla a cabo o no. Sin embargo, si en una misma conversación hay varios conocidos como, por ejemplo, compañeros de la misma empresa, y ninguno de ellos pone objeción alguna, lo más probable es que acatemos las normas, aun sin saber de dónde ni de quién provienen. Al ser las personas tan gregarias y en búsqueda permanente de la acción social, el sesgo de grupo es continuamente utilizado, también conocido como "presión grupal", especialmente en el ámbito de la política para conseguir movilizar el voto.

CONTEXTUALIZACIÓN

Luego de leer los documentos y observar el video, realice la actividad.

I.ACTIVIDAD 1:

Leer el documento y resuelve

1. En qué consiste la ingeniería social
2. Cuáles son los Principios de Mitnick
3. Explique con sus palabras, cómo se puede evitar la ingeniería social
4. Explique la caricatura de acuerdo con la ingeniería social
5. Cómo influye la ingeniería social en la vida del hombre

ACTIVIDAD 2: subir la actividad a classroom

En chatGPT busca el tema ingeniería social y tipos.

Prompt de ejemplo:

- Actua como estudiante de tecnología e informática del grado undécimo con edad entre los 15 y 16 años, crea una explicación acerca de la ingeniería social y los tipos
  - Crea el guion para un comic de 1 pestaña con 5 cuadros, que se realizara en https://llamagen.ai/

Realice un comic donde se presente un ejemplo de ingeniería social crearlo en https://llamagen.ai/

RÚBRICA. DE TECNOLOGÍA E INFORMÁTICA

Actividad tecnología e informática					
Aspectos a evaluar	ESCALA DE CALIFICACIÓN				
	4.6 a 5.0 Desempeño superior	4.0 a 4.5 Desempeño Alto	3.0 a 3.9 Desempeño Básico	1.0 a 2.9 Desempeño bajo	Porcentaje
Crea informes escritos con adecuada redacción y ortografía.	Elabora eficientemente escritos con adecuada redacción, ortografía donde se identifican el tema tratado	Elabora medianamente escritos con adecuada redacción, ortografía donde se identifican el tema tratado.	Elabora escritos con problemas de redacción, ortografía donde se identifican el tema tratado	Elabora con dificultad escritos con problemas de redacción, ortografía sin identificar el tema tratado	50%
Utiliza herramientas	Domina y utiliza herramienta de manera elevada para la elaboración de documentos	Domina y utiliza la herramienta de manera eficaz adecuada para la elaboración de documentos	Domina y utiliza la herramienta para la elaboración de documentos	Presenta dificultades para utilizar la herramienta en la elaboración de documentos.	50%
Total					100%

Fuente

Tomado de:

https://elusuariofinal.wordpress.com/2010/10/04/los-4-principios-basicos-de-la-ingenieria-social/

https://www.youtube.com/watch?v=rgqxMNn5qwc

https://www.avast.com/es-es/c-social-engineering

https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

https://colciber.co/introduccion-a-la-ingenieria-social/

https://www.incibe.es/ciudadania/formacion/infografias/el-ciclo-de-la-ingenieria-social-como-preparan-los-ciberdelincuentes-un-ataque-de-ingenieria-social

https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

https://forum.huawei.com/enterprise/es/%C2%BFqu%C3%A9-es-la-ingenier%C3%ADa-social/thread/1045236-100233

https://llamagen.ai/