Universitat Oberta de Catalunya

uoc.edu

Estudio de metodologías de Ingeniería Social

David Berenguer Serrato
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
TFM-Ad hoc

Angela María García Valdés
Victor Garcia Font

06/2018

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Estudio de metodologías de Ingeniería Social*
Nombre del autor:	*David Berenguer Serrato*
Nombre del consultor/a:	*Angela María García Valdés*
Nombre del PRA:	*Victor Garcia Font*
Fecha de entrega (mm/aaaa):	06/2018
Titulación::	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*TFM-Ad hoc*
Idioma del trabajo:	*Castellano*
Palabras clave	*Metodologías Ingeniería Social*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El trabajo consiste en un estudio sobre las técnicas de ingeniería social y los métodos usados para obtener información.
Primero se introducirá la definición, y un poco de historia, de que es la ingeniería social. Después se verán los conceptos relacionados con la ingeniería social. Y a continuación se detallarán los métodos más usados, además de descubrir qué tipo de información puede llegar a obtenerse y cómo esta es utilizada para obtener beneficios.
También se verá como defenderse o realizar un ataque con la ingeniería social, además de mencionar a grandes ingenieros notables y concluyendo finalmente en como afecta la ingeniería social y casos reales de esta.

Abstract:

The work is a study about social engineering techniques and the articles used to obtain information.
First, the definition, and a bit of history, of social engineering is presented. After seeing the concepts related to social engineering. And then see details about the most used methods, as well as discover what kind of information can be obtained and how it is used to obtain benefits.
He also sees himself as a defender or carrying out an attack with social engineering, in addition to mentioning a great engineers and finally concluding in how it affects social engineering and real cases of it.

Índice

1. Introducción 1
1.1 Contexto y justificación del Trabajo 1
1.2 Objetivos del Trabajo 1
1.3 Enfoque y método seguido 1
1.4 Planificación del Trabajo 2
1.5 Breve sumario de productos obtenidos 3

2. ¿Qué es la ingeniería social? 4
2.1 Historia de la ingeniería social 4
2.2 La evolución de las técnicas de ingeniería social 5

3. Ingeniería social y seguridad informática 5

4. Principios básicos de la ingeniería social 6
4.1 Reciprocidad 6
4.2 Urgencia 6
4.3 Consistencia 6
4.4 Confianza 6
4.5 Autoridad 7
4.6 Validación social 7

5. ¿Que roles intervienen? 7
5.1 ¿Como estudiar un rol? 8

6. Tipos de ataques de ingeniería social 10
6.1 Phishing 10
6.2 Spear Phishing 11
6.3 Vishing 11
6.4 Pretexting 11
6.5 Baiting 11
6.6 Tailgating 11
6.7 Quid pro quo 12

7. Vías de ataque de ingeniería social 12
7.1 Ingeniería social por teléfono 12
7.2 Ingeniería social por Internet 12
7.3 Ingeniería social por Dumpster Diving 12
7.4 Ingeniería social por persuasión psicológica 13

8. ¿Cómo podemos defendernos de la ingeniería social? 13
8.1 ¿Como prevenir estos ataques? 14

9. Como realizar un ataque de ingeniería social 14
9.1 Ciclo de una ataque de ingeniería social 14
9.2 ¿Cómo obtener información para el ataque de ingeniería social? 16
9.3 ¿Cómo realizar el ataque? 17

9.4 Buscando el momento perfecto 17
9.5 Proceso completo de como realizar un ataque de ingeniería social 18

10. Ingenieros sociales notables 19
10.1 Kevin Mitnick 19
10.2 Christopher Hadnagy 20
10.3 Mike Ridpath 20
10.4 David Pacios 20
10.5 Badir Brothers 20

11. ¿Como puede afectar a las empresas y personas? 21
11.1 El 50% de las empresas víctimas de la ingeniería social 21
11.2 La importancia de tomar medidas e informar 21

12. Casos reales de ataques 22
12.1 Cuando blindar sistemas informáticos no lo es todo 22
12.2 Caso Ubiquiti Networks 22
12.3 La influencia de un falso tweet en la economía mundial 23
12.4 La estafa nigeriana (o estafa 419) 24
12.5 Estafas relacionadas a muertes de celebridades 25
12.6 Falsas noticias alarmantes de Facebook 25
12.7 Fotos y videos íntimos de famosos, para los más extremos 26
12.8 WhatsApp para PC, estafa antes de realidad 27

13. Conclusiones 28

14. Bibliografía 29

1. Introducción

1.1 Contexto y justificación del Trabajo

Hoy en día muchas personas no son conscientes de que la Ingeniería Social es una realidad. Es un tema que nos afecta a todos, ya sea en el trabajo o vida personal, y dicho desconocimiento de información hace que sea un tema mas delicado. Se pretende resolver las dudas que a cualquiera se le podrían plantear al escuchar las palabras Ingeniería Social, para que de una manera unificada, comprender un poco mas todo su significado y lo que le rodea.

1.2 Objetivos del Trabajo

El trabajo consiste en un estudio sobre las técnicas de ingeniería social y los métodos usados para obtener información. Para ello habrá que familiarizarse con los conceptos relacionados con la ingeniería social, detallar los métodos más usados, descubrir qué tipo de información puede llegar a obtenerse y cómo esta es utilizada para obtener beneficios.

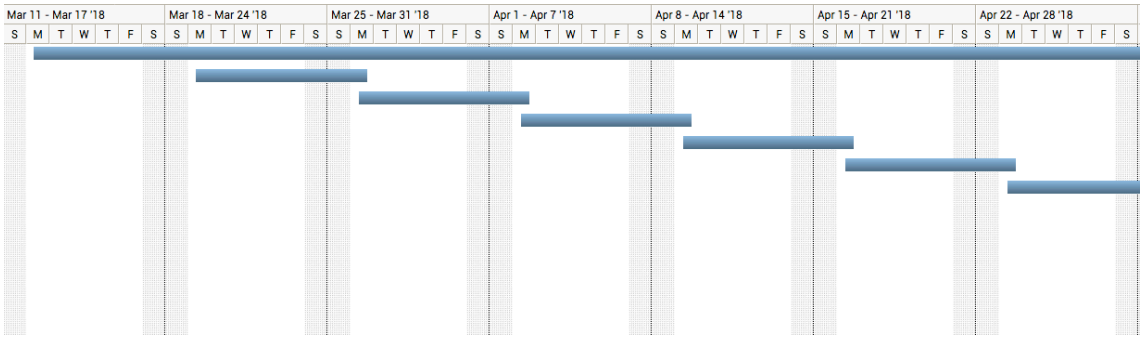
1.3 Enfoque y método seguido

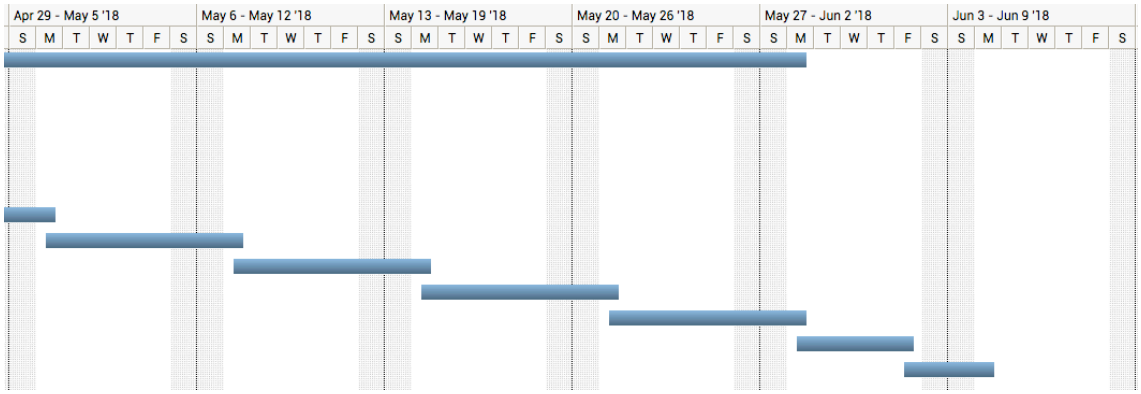
Al ser un trabajo enfocado teóricamente, la metodología empleada principalmente estará basada en la búsqueda y síntesis de la información encontrada. Siendo las principales fuentes de información libros, webs y videos.

1.4 Planificación del Trabajo

Se ha realizado un diagrama de Gantt con la planificación inicial del TFM, aunque finalmente algún punto concreto ha variado levemente.

	Name	Duration	Start	Finish
1	Busqueda de información	56days	03/12/2018	05/28/2018
2	Desarrollo del punto: ¿Qué es la ingeniería social?	6days	03/19/2018	03/26/2018
3	Desarrollo del punto: Principios básicos	6days	03/26/2018	04/02/2018
4	Desarrollo del punto: Tipos de ataques	6days	04/02/2018	04/09/2018
5	Desarrollo del punto: Ingeniería social y seguridad informática	6days	04/09/2018	04/16/2018
6	Desarrollo del punto: Como prevenir y defenderse los ataques	6days	04/16/2018	04/23/2018
7	Desarrollo del punto: Como realizar un ataque	6days	04/23/2018	04/30/2018
8	Desarrollo del punto: Como puede afectar a las personas y empresas	6days	04/30/2018	05/07/2018
9	Desarrollo del punto: Casos reales de ataques	6days	05/07/2018	05/14/2018
10	Desarrollo del punto: Legislación aplicada	6days	05/14/2018	05/21/2018
11	Desarrollo del punto: Pioneros en el ámbito	6days	05/21/2018	05/28/2018
12	Primera revisión del trabajo	5days	05/28/2018	06/01/2018
13	Segunda revisión del trabajo	2days	06/01/2018	06/04/2018





1.5 Breve sumario de productos obtenidos

Los puntos que se han desarrollado finalmente han sido los siguientes:

- ¿Qué es la ingeniería social?
- Ingeniería social y seguridad informática
- Principios básicos de la ingeniería social
- Que roles intervienen
- Tipos de ataques de ingeniería social
- Vías de ataque de ingeniería social
- Como podemos defendernos de la ingeniería social
- Como realizar un ataque de Ingeniería Social
- Ingenieros sociales notables
- Como puede afectar a las personas y empresas
- Casos reales de ataques

2. ¿Qué es la ingeniería social?

Se puede definir como el conjunto de técnicas o estrategias sociales utilizadas de forma premeditada por un usuario para obtener algún tipo de ventaja respecto a otro u otros. Por lo que de ingeniería tiene más bien poco, es más, de hecho se acerca más a la psicología social o la sociología de ventas. Ya que para llevar a cabo ataques de ingeniería social, no tienes porqué tener conocimientos técnicos de ningún tipo.

Todo ello implica que en la práctica no haya ningún sistema informático que nos pueda prevenir de un ataque de este estilo. Como mucho, la implantación de directivas de seguridad, ISOs o normativas, que eviten que el eslabón más débil de la cadena, el trabajador/cliente/usuario, tenga los permisos y conocimientos suficientes como para caer en un engaño, o al menos para minimizar las consecuencias asociadas a él.

Se suele obtener información de los usuarios normalmente mediante teléfono, correo electrónico, webs, correo tradicional o contacto directo. Los atacantes de la ingeniería social usan la fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, un técnico o un administrador, etc.

En general, los métodos de la ingeniería social están organizados de la siguiente manera: una fase de acercamiento para ganarse la confianza del usuario, haciéndose pasar por un integrante de la administración, de la compañía, un cliente, proveedor, etc.; una fase de alerta, para desestabilizar al usuario y observar la velocidad de su respuesta. Por ejemplo, este podría ser un pretexto de seguridad o una situación de emergencia; una distracción, es decir, una frase o una situación que tranquiliza al usuario y evita que se concentre en la alerta. Podría ser un agradecimiento que indique que todo ha vuelto a la normalidad, una frase hecha o, en caso de que sea mediante correo electrónico o de una página web, la redirección a la página web de la compañía.

2.1 Historia de la ingeniería social

El uso de la expresión se inició en 1894 con un ensayo del empresario y filántropo holandés J.C. Van Marken, difundido en Francia por Émile Cheysson (uno de los integrantes del Musée Social), pero recibió su mayor impulso en EE.UU. a través del libro "*Social Engineering*" del reformista social W.H. Tolman, conocido en aquella época por "ayudar a los pobres". La idea central es que no había en las empresas una función social (algo así como los departamentos de recursos humanos de hoy), por lo que el ingeniero social tenía una función de mediador para resolver los conflictos como intermediador racional entre el capital y el trabajo. En esta acepción, el ingeniero social debía contar con habilidades sociales, en contraste con el uso posterior del término, basado en la metáfora de la máquina que se convierte en el núcleo del concepto peyorativo actual.

Se sugiere que el origen del término está en el concepto filantrópico de los pensadores liberales de la segunda mitad del siglo XIX como los "intermediarios racionales" entre el capital y el trabajo. Para las décadas 30 y 40 del siglo XX el término había caído en desuso.

A partir de esta especialización, se generaliza el concepto de que la ingeniería social puede ser una técnica o método para lograr una variedad de resultados, es decir, deja de ser un instrumento para resolver problemas sociales y se transforma en uno para manipular a la población. Es evidente en este punto que la propaganda puede ser considerada ingeniería

social, así como las campañas políticas y la religión, dado que buscan lograr un comportamiento específico en las masas. En 1945 Karl Popper reintroduce el término con la acepción de implementación de métodos críticos y racionales de la ingeniería y ciencia a los problemas sociales

2.2 La evolución de las técnicas de ingeniería social

Es increíble ver cómo han evolucionado hasta la fecha los ataques de este tipo. Algo que en sus inicios comenzó siendo una impersonalización vía telefónica**,** hoy busca hacer una experiencia imperceptible al usuario.

Los comienzos de esta técnica se basaban en llamadas telefónicas, haciéndose pasar por entidades que brindan un determinado servicio. La finalidad de este llamado era recabar información sobre la víctima. Con la llegada de Internet a cada hogar, comenzaron a aparecer técnicas de Ingeniería Social vía clientes de mensajería instantánea. Comenzó a ser muy común el famoso mensaje mediante Messenger *"Fotos_para_adultos_de_alguien.rar".* Enviando código malicioso a los contactos de la cuenta, hubo muchos casos de infección mediante esta técnica.

Hoy en día, los ciberdelincuentes buscan engañar a sus víctimas para que entreguen voluntariamente su información personal. La mutación se dio no sólo hacia sitios *web*, sino también se ha transformado en mensajes de texto, y cualquier tipo de mensajería móvil. La importancia de este vector de ataque radica en que estos dispositivos móviles almacenan gran cantidad de información personal, como contactos, fotos, conversaciones, usuarios y contraseñas de redes sociales, de correos electrónicos, inclusive geo localización.

3. Ingeniería social y seguridad informática

Muchos nos hemos puesto a resolver test, descargar aplicaciones, contestar formularios y muchas otras cosas que nos ofrecen a través de las redes sociales y como solemos no leer advertencias, damos datos o permitimos que la información de nuestras cuentas sea accedida por piratas informáticos o por app que a las que incluso les autorizamos a publicar por nosotros.

El elemento de manipulación social a través de nuestras conductas e intereses en las redes sociales, es un camino dorado para el robo de información clave de nuestros productos y vulnera nuestra seguridad, incluso podríamos hablar hasta de nuestra integridad física, toda vez que hay muchos delincuentes informáticos o bandidos que se valen de la huella que dejamos en la red para cometer delitos contra las propiedades o contra las personas. Si bien no se trata de ser paranoico, si debemos tener en cuenta los riesgos latentes y estar conscientes de ello.

La ingeniería social consiste en el diseño de estrategias para manipular psicológicamente a los usuarios de internet para que compartan información confidencial o cometan errores al realizar operaciones inseguras y queden expuestos a través de esa metodología.

Seguramente todos hemos recibido alguna vez un correo que nos dice "Querido mío" y te echan un cuento en el que alguien en algún lugar quiere donar su fortuna y todo eso y que solo debes dar los datos de cuentas bancarias. Uno cree que no existe gente que pueda caer en una trampa tan tonta, pero los hay y muchos, por algo existen esos mensajes. Si no hubiese quien cayera en eso, pues no tendrían sentido. ¿A qué apela eso? Pues a la necesidad de las personas. Y no hay una vía más expedita para engañar a alguien que haciendo uso de las necesidades. Siempre el deseo de tener aquello que me hace falta nos lleva a actuar muchas veces de manera irracional.

4. Principios básicos de la ingeniería social

Como toda materia, tiene algunos elementos básicos con los que un criminal juega para ganarse el respeto o confianza suficiente y engañar a la víctima. Y casualmente se parecen mucho a los principios básicos de las ventas, ¿casualidad?

4.1 Reciprocidad

Los humanos somos por naturaleza recíprocos con nuestros actos. Si alguien nos ofrece algo, tendemos a ofrecerle también algo nosotros. Si alguien nos trata mal, estaremos más susceptibles a pagarle con la misma moneda. Un "instinto" social muy arraigado en nuestra naturaleza, y por ende, fácilmente manipulable. *La próxima vez que alguien le ofrezca un trabajo de ensueño desde su casa en el que solo tiene que meter dinero de una cuenta a otra y se queda un % por cada transacción, desconfíe. Si es tan sencillo de hacer, ¿por qué no lo hacen ellos?*

4.2 Urgencia

Un clásico entre los clásicos. *¡Aproveche esta oferta! ¡Hasta fin de existencias! ¡Durante los próximos cinco minutos…!* Es uno de los mantras habituales de las ventas, en este caso extrapolado al cibercrimen. La mayoría de los ataques de ingeniería social, enganchan a las víctimas por medio de la urgencia. *Tienes 24 horas para enviarme X datos del banco o Hacienda te pondrá la consabida multa. Comparte ahora mismo este artículo entre todos tus contactos de Facebook y ganaras 100 de oro para gastar en esta aplicación…* ¿seguimos?

4.3 Consistencia

Somos animales de costumbres. Si hemos dado nuestra palabra, tendemos más a cumplir que a no hacerlo. El caso de ingeniería social más habitual utilizando este principio es aquel en el que *un miembro del equipo técnico de un servicio (o de una empresa) le pide que realice X labores habituales. Aunque una de ellas sea "rara de cojones", como ya se ha comprometido la acabará haciendo junto al resto. Y el criminal ya tendrá seguramente acceso a los servicios de la compañía en su nombre.*

4.4 Confianza

Nuestras escasas defensas bajan cuando nuestro interlocutor nos cae bien o está alineado con nuestros intereses. Por no hablar de nuevo de la novia rusa, no es raro que *altos directivos o trabajadores con acceso a contenido o servicios confidenciales (gobierno, corporaciones, política, militar,…) sean "seducidos" por supuestos perfiles semejantes (no*

tienen porqué ser del sexo opuesto, aunque tiende a ayudar) que se ganan su confianza lo suficiente como para que tengan un descuido y puedan aprovecharse de él. A continuación es cuando esa chica morena, ejecutiva de cuentas de X institución, se transforma en un maromo del este que le extorsiona con desvelar contenido inapropiado enviado la noche anterior sino cumple al milímetro sus exigencias.

4.5 Autoridad

Si el becario le pide las credenciales de acceso de un servicio, seguramente lo mire con desconfianza. Pero si quien lo hace es el jefe, *la cosa cambia.* La usurpación de identidad juega un papel decisivo, bien sea real (robo del perfil digital del jefe) o aparentada (clonado de perfiles o emails muy parecidos).

4.6 Validación social

Como seres sociales que somos, buscamos la aprobación del colectivo. Por tanto, si en un email alguien nos pide específicamente que hagamos algo raro, es posible que nos lo pensemos. Pero si en esa misma conversación hay varios conocidos más (*por ejemplo trabajadores de la misma compañía*), y ninguno rechista, entenderemos que no hay ningún problema y acataremos las normas, vengan de quien vengan.

5. ¿Que roles intervienen?

A continuación vamos a ver como asumir uno o varios roles en los distintos escenarios que se puede encontrar un experto ingeniero social.

Para ello es necesario crear un escenario inventado para persuadir a la víctima divulgando información confidencial o realizando alguna acción como por ejemplo dar la contraseña del administrador de alguno de los servidores de la organización, o dándole acceso a una planta de acceso restringido del edificio.

Esto es mucho más complejo que crear una simple mentira. La mentira puede llegar a convertirse en una nueva identidad, muy usado en la películas de espionaje. Tenemos:

- **Escenario**: Donde se desarrollarán las operaciones. Puede ser físico o lógico.
- **Identidad**: Necesaria como parte de nuestro rol. Una nueva identidad garantiza anonimato, accesibilidad y viabilidad en los diferentes escenarios que el experto ingeniero social se pueda encontrar.
- **Rol**: Esta ligado a lo anterior. Con un rol, tendrás una identidad y se actuará en un escenario acorde al rol elegido. Es usado para manipular u obtener información privilegiada de la víctima. En el ámbito de la ingeniería social es muy usado para hacerse pasar por un miembro de la organización empresarial interpretado.

No sólo puedes asumir un rol, sino cuantos más roles se pueda asumir, más información podrá recabar en los diferentes escenarios de cada rol.

Esto requiere mucho tiempo de estudio, ya que el preparase dos roles implica tener varias identidades y especializarse en dos campos técnicos del rol, como puede ser la informática y

las relaciones públicas. Por tanto la preparación del rol es importante para poder imitar a la perfección la nueva identidad. Por ejemplo, imitar y actuar igual en cuanto a los conocimientos se refiere de un técnico informático de una organización empresarial inspirando confianza y afabilidad. Con afabilidad nos referimos donde la unión de las dos temáticas proporciona que las personas se sientan cómodas dando información a su atacante sin sospecha en el escenario creado.

Para garantizar la identidad anónima, existen muchos métodos lógicos (a través de la red) como *Tor* o *I2P*, preservando la huella digital "intacta". Y físicos con la creación o falsificación de pasaportes muy vistos en las películas de espionaje.

5.1 ¿Como estudiar un rol?

Para que el experto ingeniero social, tenga éxito en su operación, es necesario una perfecta planificación y estudio sobre el rol que va a desempeñar. Hay que tener en cuenta que muchas de las características previas a la operación son innatas, es decir no se pueden aprender desde cero, pero si perfeccionarlas. *"El perfecto ingeniero social no se crea, sino se mejora".*

Para ello, el arduo perfeccionamiento de estas técnicas sociales y psicológicas requiere de mucho tiempo y confianza en si mismo. Dependiendo del rol empeñado, el ingeniero social actuará de la misma forma que lo haría un miembro de la organización o empleado externo a ella. El lenguaje corporal y verbal, toma gran protagonismo en este ámbito. Por ejemplo la forma de sentarse, de hablar, de moverse, la vestimenta, etc.

La investigación de fuentes abiertas (OSINT) y otros métodos de obtención de información como (HUMINT) es vital para tener más éxito en la creación del rol. *"Información es poder"*. Con toda esta información podremos realizar un esquema o mapa conceptual de las posibles dificultades que nos podemos encontrar en la aplicación del rol en el escenario. Se podría decir que aplicamos inteligencia a la creación del rol, que es muy distinto a la información y posterior análisis y creación de inteligencia obtenido con la aplicación del rol.

Dependiendo de la zona geográfica, el acento y expresiones empleadas como parte de la conversación de forma espontánea puede llegar a influir negativamente si no se ha tomado en cuenta en el estudio del rol como práctica. Este estudio del acento o incluso dialectos es muy importante, ya que el escenario donde se desarrolle la acción puede verse envuelto con personas que hablen con ese acento y la conversación y todo el plan puede verse perjudicado y levantar sospechas si no se tiene en cuenta. Para ello la solución es como siempre, practicar con sesiones y convertirse en un perfecto actor. Si no eres natural es muy difícil que se pueda llevar a cabo estas sesiones con excelentes resultados. Por eso lo que antes se ha mencionado, el ingeniero social se perfecciona no se crea, son perfectos actores. Si no se dispone de personas en la cual se pueda practicar estas sesiones, siempre se puede grabar la voz del contexto textual, y escucharla luego para realizar un análisis del resultado. Escuchar la radio o la televisión de la zona geográfica o ámbito adquisitivo en cuanto a las expresiones coloquiales que se usan, es también una solución para practicar.

Muchas veces entra en discusión sobre la simplicidad del rol a tomar. No tiene porque ser más efectivo si es simple el rol, sino el dominio de él.

Es importante un estudio técnico del rol a desempeñar para evitar que salga mal el plan. El tema técnico especifico se refiere a dominar la informática si el rol es un administrador

de sistemas informáticos, o de derecho si el rol es ser un abogado...y muchas más disciplinas. Si se tiene especial interés en alguna de estas disciplinas, será un punto más a favor. La información para documentarse se puede encontrar en cursos, páginas web o libros.

Un buen ingeniero social que realiza un estudio minucioso de su rol sabe perfectamente enmascararse en su perfil haciendo creer a su víctima, inspirándole confianza por sus actitudes y acciones, y en definitiva su conocimiento técnico en la disciplina del rol elegida.

La presión inspira nerviosismo al ingeniero social. Para ello es necesario el perfeccionamiento de esta técnica haciéndose pasar el que usa este rol como instructor y el novato ingeniero social. Un ejemplo sería que el instructor haya conseguido acceso físico a una empresa, y este atento a su compañero para que este le pida el identificador de empleado o el número de teléfono de cierta persona y este pueda valorar mediante las facciones corporales y verbales si esta nervioso.

El uso del teléfono móvil para realizar ataques de ingeniería social, es un hecho muy importante como parte del estudio del rol. No requiere presencia física en el lugar y se puede obtener gran cantidad de información valiosa. Digamos que es positivo, ya que al no tener contacto físico con la persona con la que forma parte en la conversación:

- No puede analizar el lenguaje corporal y no saltar alertas de sospecha
- No se expone ante medios de vigilancia de seguridad en la organización empresarial

Tiene una desventaja. Un perfecto "actor" o ingeniero social, si se vale de su encanto y su lenguaje corporal puede obtener más información de la víctima causándole afabilidad, empatía y confortabilidad.

La complejidad en el estudio del rol se puede hacer patente dependiendo del escenario donde se ponga en practica. Cuanto más complejo sea el rol, más posibilidades de fallo en la operación. Este si es sencillo se conseguirá más facilidad de recuerdo. Un rol complejo viene definido en el estudio dedicado previo. La preparación es primordial.

Ejemplos de roles, tenemos muchos y dependiendo de la disciplina tenemos a expertos ingenieros sociales que se hacen pasar por altos ejecutivos, a un simple técnico de mantenimiento.

En el caso de un técnico solo nos vale vestir con un polo de la empresa y un portátil en muchas ocasiones con gran facilidad de acceso físico y sin supervisión. Para empezar nuestro rol basta con decir:

Atacante: *"Soy el técnico informático de la empresa X"* (Puesta en marcha del rol)
Víctima: *"Claro, y ¿cuál es la tarea que va a realizar?"* (Se hace patente y realidad el escenario)
Atacante: *"Vengo a realizar el mantenimiento de los servidores"* (Plan técnico del rol)
Víctima: *"Muy bien, ¿me deja su tarjeta de empleado para verificarlo en la BBDD?"*
Atacante: *"Si, claro por supuesto"* (La obtención de información previa, y falsificación de nuestra identidad)

Toda conversación que vaya a formar parte en nuestro plan, debe ser espontánea:

- No puede influir el que se haya preparado el rol durante 2 semanas o más en nuestro comportamiento y se pierda credibilidad debido a expresiones frías y con poca naturalidad.
- Ciertas expresiones tales como *eeee* o *ummm* en la conversación implica inseguridad y aparenta cierta desconfianza y poca empatía con la víctima en este caso.
- Saber identificar en la conversación, trozos de información de gran relevancia, para su posterior análisis y obtención de inteligencia.
- No hay que ser muy serio, tener notas de humor de vez en cuando y desvelar una bonita sonrisa causa simpatía y afabilidad.
- Los tiempos de respuesta influyen mucho también.

La fase culmen del perfeccionamiento, y puesta en práctica de los dotes de un experto ingeniero social en la realidad, es de vital importancia. O lo que es lo mismo, ser un ingeniero social con experiencia. Para ello se puede poner en práctica con la familia, amigos, con desconocidos, con uno mismo, etc.

6. Tipos de ataques de ingeniería social

Primero podemos considerar que hay dos grandes grupos dentro de la ingeniería social:

- **Hunting:** Son aquellos ataques que buscan obtener información específica del objetivo con la menor exposición directa posible. Con el menor contacto. En la práctica hablamos de ataques de ingeniería social enfocados a obtener X dato (*normalmente credenciales de acceso a un servicio o cuenta, activación o desactivación de alguna configuración que puede complicar el objetivo final o como apoyo a un ataque mayor, dirigido y persistente*), de forma que el atacante se pone en contacto de alguna manera con la víctima, y la insta a realizar una acción cuyo desenlace es el pretendido inicialmente. Y el mejor ejemplo son las campañas de phishing por email, en el que únicamente se suele tener contacto directo con el cibercriminal una sola vez (*el email que te envía haciéndose pasar por una entidad o conocido, habitualmente para que insertes tus datos en una supuesta web legítima*).

- **Farming:** Pues justo lo contrario. En el *hunting* lo que se busca es una exposición mínima. Obtener algo y desaparecer. Con el *farming* el objetivo es mantener el engaño el mayor tiempo posible, para exprimir al máximo el conocimiento, recursos o posición de la víctima. Para ello, se suele recurrir a granjas de identidades, que por lo general han sido robadas con anterioridad. *Esa novia rusa que se enamora de ti después de haberte visto por alguna red social, ese príncipe nigeriano sin descendencia que casualmente te ha elegido entre los miles de millones de personas de todo el mundo para que heredes su numerosa fortuna… eso sí, después de pagar unos mínimos costes de aduana/retenciones fiscales/seguros,…*

6.1 Phishing

El *phishing* es el tipo más común de ingeniería social. El atacante hace una copia del sitio web (en la mayoría de ocasiones la parte del soporte técnico) de una empresa reconocida y envía el enlace a los objetivos a través de correos electrónicos o mediante redes sociales. La

persona, desconociendo el verdadero objetivo del atacante, termina por comprometer información personal e incluso detalles de tarjetas de crédito.

6.2 Spear Phishing

La técnica de ingeniería social conocida como *spear phishing* se considera como un subconjunto del *phishing*. Aunque son similares, se requiere un esfuerzo adicional desde el lado del atacante. Tiene que prestar atención al grado de singularidad para limitar el número de usuarios a los que se dirige. Este trabajo duro da sus frutos; las posibilidades de que los usuarios que caigan en los falsos mensajes de correo electrónico son considerablemente mayores con esta técnica.

6.3 Vishing

Los impostores o ingenieros sociales pueden estar en cualquier lugar de Internet. Pero muchos prefieren la manera antigua, utilizar el teléfono. Este tipo de ingeniería social se conoce como *vishing*. Ellos recrean el sistema IVR (Respuesta de Voz Interactiva) de una empresa. Se adhieren a un número de teléfono gratuito y engañan a la gente llamando a su número. La mayoría de la gente no piensa dos veces antes de ingresar información confidencial en el sistema IVR.

6.4 Pretexting

El *pretexting* es otra forma de ingeniería social, se basa en un escenario con guion presentado delante de los objetivos. Se utiliza para extraer información de identificación personal o alguna otra información. Un atacante podría hacerse pasar por otra persona o una figura conocida. Es posible que hayas visto varios programas de televisión y películas, en donde los detectives utilizan esta técnica para entrar en lugares donde no están autorizados o extraen información engañando a la gente. Otro ejemplo de esta técnica pueden ser correos electrónicos falsos que recibes de tus amigos solicitándote dinero. Si fuese este el caso, probablemente alguien hackeó su cuenta o creó una falsa.

6.5 Baiting

El baiting (cebo) es una de las técnicas de ingeniería social utilizada por gente con fines maliciosos. Los atacantes dejan unidades USB infectadas o discos ópticos en lugares públicos con la esperanza de que alguien lo recoja por curiosidad y lo use en sus dispositivos. Un ejemplo más moderno de esta técnica se puede encontrar en la web. Te encuentras diferentes enlaces de descarga (sobre todo en páginas tipo warez) que en su mayoría contienen software malicioso, estos enlaces se muestran a la gente al azar esperando que alguien haga clic en ellos.

6.6 Tailgating

Esta técnica de ingeniería social, se basa en solicitar la ayuda de una persona autorizada para tener acceso a las áreas restringidas donde está presente la autenticación de

RFID (identificación por radiofrecuencia) o alguna otra barrera electrónica. También muy utilizada en series y películas detectivescas.

6.7 Quid pro quo

Este método involucra a las personas que prestan soporte técnico. Hacen llamadas al azar a los empleados de una empresa solicitando ayuda con respecto a un tema. A veces, estas personas tienen la oportunidad de hacer que la víctima haga lo que quieren. Se puede utilizar también para la gente normal. *Quid pro quo* implica un intercambio de algo con el objetivo, por ejemplo, el atacante trata de resolver un problema real de la víctima. El cambio puede implicar cosas materiales como un intercambio de información.

7. Vías de ataque de ingeniería social

Por lo general, los ingenieros sociales utilizan el teléfono, Internet, técnicas de persuasión psicológica o Dumpster Diving para convencer a otras personas de que divulguen información confidencial o hagan algo que vaya contra sus prácticas habituales. De esta forma, explotan la tendencia natural de una persona a confiar en lo que le dicen, en lugar de explotar vulnerabilidades en sus computadoras. Lo que hace posible la ingeniería social es el principio, generalmente admitido, de que "los usuarios son el eslabón más débil" en la seguridad.

7.1 Ingeniería social por teléfono

La forma más habitual de ingeniería social es la que se realiza por teléfono. El atacante llama y se hace pasar por una persona importante para la empresa o por un consultor externo que trabaja para la empresa. Con frecuencia sigue distintos guiones que ha ensayado previamente. El atacante se gana la confianza de los clientes para conseguir de ellos información importante. Si el cliente no tiene claro qué información puede divulgar, el atacante puede aprovechar este desconocimiento para obtener más información.

7.2 Ingeniería social por Internet

La ingeniería social en Internet puede adoptar formas muy variadas. Es frecuente que el atacante envíe directamente al cliente un correo electrónico en el que le solicita su contraseña. También puede enviarle un archivo adjunto con un malware que registra las teclas que pulsa el cliente y las envía automáticamente al atacante por correo electrónico. En otras ocasiones, el archivo adjunto instala una ventana emergente que imita la ventana en la que el cliente tiene que escribir su nombre de usuario y su contraseña, lo que permite al hacker hacerse con esta información.

7.3 Ingeniería social por Dumpster Diving

Una forma menos glamorosa de ingeniería social recibe el nombre de Dumpster Diving o "búsqueda en la basura". En este caso, el atacante obtiene información sobre el cliente o la

empresa buscando en la basura que éstos han tirado. La basura de un cliente o empresa puede ser una auténtica mina de oro en la que el atacante encuentra la información necesaria para iniciar otra forma de ataque, como la ingeniería social por teléfono.

7.4 Ingeniería social por persuasión psicológica

La persuasión psicológica se puede combinar con cualquiera de las formas de ingeniería social anteriormente descritas. Es frecuente que el atacante recurra a la persuasión para ganarse la confianza del cliente, algo que resulta especialmente útil en las llamadas fraudulentas.

8. ¿Cómo podemos defendernos de la ingeniería social?

La pregunta del millón. Y la respuesta es que no hay un método infalible. Cualquiera, absolutamente cualquiera, es susceptible de caer en un ataque de ingeniería social. Da igual que sea *el panadero de la esquina*, o *Edward Snowden*. Si el ataque es lo suficientemente meticuloso, lo suficientemente sofisticado, cualquier persona va a caer.

Ahora bien, afortunadamente la mayoría de ataques son toscos, impersonales y masivos. Y aquí no hay excusa que valga. Ahora que ya conocemos los principios básicos de la ingeniería social, se trata de contrarrestarlos.

Este tipo de ataques vienen cuando menos lo esperas, por lo tanto es necesario estar alerta cuando alguien te pide que le des tu información o cuando alguna persona desconocida te está dando algo de forma gratuita. Las personas ya no son tan ingenuas como antes y los atacantes lo saben – ahora no es común ver la famosa ventana emergente diciéndote que *has ganado un millón de dólares por ser el visitante # 1000,* pues casi nadie caería en esto, pero ello implica que los atacantes han evolucionado – llevan a cabo ataques más sofisticados.

Los ingenieros sociales también pueden tratar de tocar la parte emocional de las personas. Puede que intenten llevarte en un viaje de culpabilidad, volverte nostálgico, o incluso tratar de impactar negativamente. La situación se vuelve alarmante; la gente tiene la tendencia a abrirse frente a los que tratan de darles apoyo emocional.

Una cosa más a la que hay que estar atento para salvarse de diferentes tipos de engaños de ingeniería social es lo que haces en internet. Una persona que intenta hackear tu cuenta en línea puede ver a través de tu perfil en Facebook y encontrar algunas pistas sobre las respuestas a las preguntas de seguridad o incluso tu contraseña.

En la mayoría de casos, estas preguntas se responden con cosas menos importantes como nombres de mascotas, nombres de escuela, lugar de nacimiento, etc. También presta atención a las páginas web que visitas o qué archivos descargas. Pueden contener herramientas maliciosas para recolectar tu información.

No obstante, estas son formas generales de defenderse ante un ataque de ingeniería social. Las grandes organizaciones han ideado métodos más formales para hacer frente a estas

situaciones. Esto puede incluir cosas tales como la realización de ejercicios regulares de los empleados, la capacitación para hacer frente a este tipo de situaciones y el establecimiento de métodos adecuados para identificar una persona legítima de una falsa.

Javier Perea, Director Regional de Intel Security España, decía recientemente en un estudio:

"Las amenazas de ingeniería social son peores que el malware más intrusivo, ya que es más difícil protegerse frente a ellas. Especialmente porque el objetivo son las personas, no solo el sistema. En este sentido, la forma más eficaz de protegerse frente a estas amenazas es estar informado, y las empresas deben impulsar la educación en materia de seguridad, con el fin de mitigar los riesgos."

Añadiría además el usar el sentido común en todos y cada uno de los supuestos diarios en los que nos encontremos. Como ya sabe, si algo huele mal, posiblemente es que esté podrido.

8.1 ¿Como prevenir estos ataques?

El principal consejo que se puede dar es, cuando alguien te pide algún tipo de información personal**,** verificar siempre que sea real. Si recibes un correo del banco, llama para confirmar que son ellos. Nunca reveles contraseñas, claves o nombres de usuario, especialmente por escrito y evita anotarlos. Y, por muy buena persona que parezca ese desconocido que te llama por teléfono, desconfía de él.

Existen unas medidas básicas de prevención ante estos ataques:

1) Verificar que las páginas que visitamos sean legítimas mirando que la dirección de la misma no tenga algún carácter de más o menos. Si los certificados de la página están presentes y sin válidos siendo estos HTTPS.

2) No dar ningún dato personal, bancario, etc. por teléfono. En caso de recibir una llamada del Banco (supuesto o Real) no dar información. Para eso tienen sucursales por lo que es más seguro dirigirse a una de ellas para realizar cualquier operación o actualización de datos.

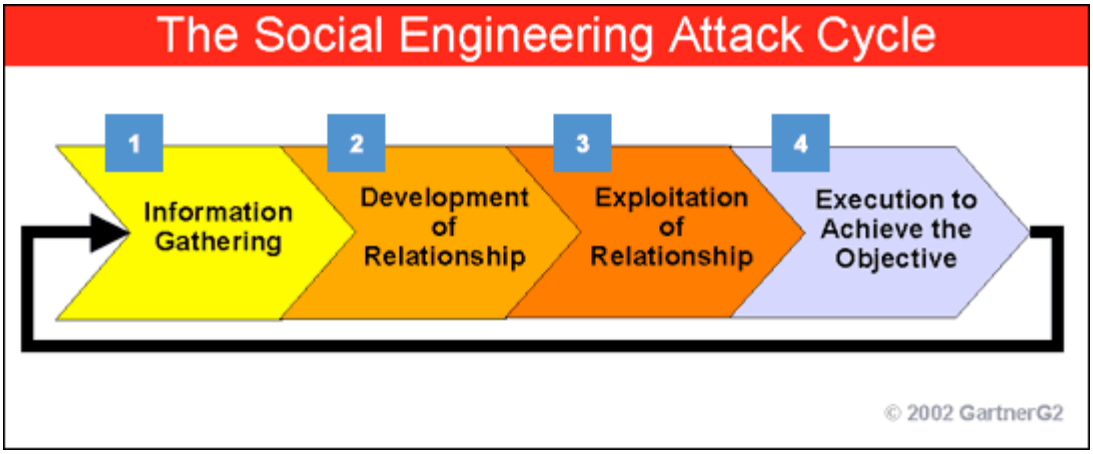
3) No descargar archivos adjuntos si el remitente es desconocido. En caso de sospechar o no tener la seguridad de su procedencia podría ser ejecutado en un SandBox.

4) En cuanto a las redes sociales no agregar a desconocidos o en caso de hacerlo verificar la configuración de seguridad para determinar que tipo de información es visible para cierto usuario.

5) Lo más importante... **Nunca se sabe quien esta del otro lado…**

9. Como realizar un ataque de ingeniería social

9.1 Ciclo de una ataque de ingeniería social



Indudablemente, las líneas siguientes no aspiran a dar una fórmula de los pasos a seguir en esta metodología de intrusión. Sino más bien una especie de sistematización de elementos comunes y lógicos cuando se desarrolla la misma en un ataque "puro" a la víctima. La pericia y experiencia del que realiza el engaño, y las particularidades del objetivo incidirán directamente en los resultados.

Se habla así de las siguientes etapas:

1. Selección y reconocimiento: implica selección y recolección de información acerca de la víctima u objetivo. Es indispensable saber el escenario que se pretende atacar. No es lo mismo obtener una contraseña de un gerente de una empresa, que información sobre seguridad militar. Seguramente en el primer caso, un recorrido por las redes sociales brindará (voluntariamente) información para ser usada en un ataque de ingeniería social. Aquí se comienza realizar un perfil de la víctima: confiado, expuesto, con conocimientos informáticos o no, etc.

2. Análisis y contacto: la información obtenida en la fase anterior, se examina cuidadosamente. El siguiente paso será el contacto con el objetivo mediante a cualquiera de los mecanismos que comentamos en el apartado anterior. Esta fase es de vital importancia, se comienzan a generar los vínculos, se construye la relación de confianza y se va “ascendiendo” en la relación que llevará a la víctima revelar la información deseada.

3. Generación de vector de ataque y explotación: el vínculo de confianza se ha creado. La psicología del humano está en la fase de auge en materia de manipulación. Los elementos recolectados en las dos etapas anteriores, habilitan a derrotar “defensas”, y así arribar a la etapa final.

4. Ejecución de vector e intrusión: éxito del ataque. Finalmente se han obtenido los datos sensibles del objetivo que permiten vulnerar su seguridad: acceso a una cuenta, al sistema, red, etc.

Estas son líneas generales, los llamados ataques mixtos, son también cuidadosamente planificados y estructurados; y comprenden toda la información que se expone en línea, por ejemplo, las transacciones comerciales; que implican no solo un engaño a la víctima sino la propia vulnerabilidad del sitio Web y el uso de herramientas automatizadas.

9.2 ¿Cómo obtener información para el ataque de ingeniería social?

Durante la fase de reconocimiento, se reunirá toda la información sobre su objetivo como sea posible. La siguiente es una lista de algunas de las herramientas utilizadas por los expertos de *International Institute of Cyber Security iicybersecurity*, una empresa de seguridad de la información:

- **Google** – Buscar en Google la empresa, buscando en el directorio de empleados, buscar en Google los nombres de los empleados y excavar de forma gradual saca una montaña de información.
- **Maltego** – Maltego es una poderosa herramienta para recopilar, combinar y analizar OSINT sobre un objetivo. Es una excelente plataforma para reunir y analizar OSINT.
- **Whois** – Whois te dirá quién es dueño de un dominio. Si una empresa está en la mira, el administrador del dominio de la empresa frecuentemente aparece con su número de teléfono o un número para el departamento de TI.
- **Twitter, Facebook, LinkedIn, FriendFinder** y otros sitios sociales o sitios con perfiles públicos pueden revelar una gran cantidad de conocimientos acerca de un individuo o una empresa. Los empleados de la compañía pueden revelar detalles acerca de la estructura de empresa, horarios, nombres de compañeros, explican expertos de empresa de seguridad de la información.
- **Google Imagenes** – Esto es lo primero que enseñan en un curso de seguridad de la información. Una característica poco conocida de imágenes de Google es la capacidad de rastrear una foto de perfil en una búsqueda de Google imágenes. Si usted puede encontrar una foto de perfil pública para un individuo, trate de rastrear en búsqueda de imágenes de Google.
- **PiPl.com** – Este servicio puede ser un poco atemorizante. Otro servicio que sorprenderá de la cantidad de datos manejados.
- **Shodan** – Shodan es un increíblemente potente motor de búsqueda de la red. Se va alrededor de la indexación qué los servicios que están escuchando en los puertos de red. Se puede proporcionar, por ejemplo, una lista de los routers Cisco de escucha en un puerto en particular de rango de direcciones IP de una empresa.
- **TinEye** – Acuerdo a curso de seguridad de la información es una búsqueda de la imagen inversa que también es útil para buscar fotos de perfil que coincidan con una foto existente. Revela perfiles de usuarios alrededor de la red.
- **Archive.org** – También se llama WayBackMachine, es una de herramientas favoritas de empresas de seguridad de la información. Esto permite ver las versiones anteriores de una página web, a menudo se remonta a varios años. Esto puede proporcionar nombres de los empleados anteriores que ya no está con la empresa, o la inteligencia en las actualizaciones de sitio y los cambios.
- **Monster.com, GlassDoor, Indeedy** otros sitios web relacionados con el empleo pueden proporcionar una gran cantidad de información en sus descripciones de trabajo. Se puede aprender sobre qué hardware y software una empresa está utilizando, qué nivel de autorización de seguridad de la información los empleados tienen y más.

Estas son sólo algunas de las herramientas que los ingenieros sociales utilizan para recopilar datos sobre un objetivo.

9.3 ¿Cómo realizar el ataque?

A continuación estas serían algunas de las formas en las que un ingeniero social buscará cómo se puede utilizar la información:

- Los nombres de los empleados: "Hola, ¿Puedo hablar con Bob Simmonds?"
- Sus nombres colega: "Hola Bob, esta es Mary de TI. Acabo de hablar por teléfono con MattSmith".
- Lo que sus colegas están haciendo: "Matt está enfermo hoy…"
- Ubicación de las mesas personales: ". … Pero estoy seguro de que sabes que ya que ustedes comparten un cubículo"
- Los nuevos despliegues de tecnología en una empresa: "Yo quería saber cómo esa nueva estación de trabajo está trabajando para usted."
- ¿Qué tecnología se está utilizando: "Yo sé que Windows 10 no es el favorito de todos, pero espero que la nueva versión de Office te está ayudando"

En este punto, se está convencido de que podría solamente estar hablando con un empleado interno porque ya se sabe mucho. Probablemente se va a compartir información libremente con esta persona.

9.4 Buscando el momento perfecto

Ahora bien, pensemos cómo un ciberdelincuente logra (o intenta lograr) que su campaña de propagación de amenazas tenga éxito.

Uno de los factores más aprovechados son las temáticas populares de actualidad. En el Laboratorio de Investigación de ESET Latinoamérica, se han podido detectar e investigar campañas que utilizaron noticias, personas y sucesos de relevancia como gancho para captar víctimas. Estas fueron algunas de las campañas destinadas a usuarios de Latinoamérica:

- Mundial de fútbol Brasil 2014: una campaña buscaba robar información bancaria prometiendo entradas para asistir a los partidos de la Copa.
- Supuesto video íntimo de la hija de Sebastián Piñera: un correo electrónico promocionaba un video de Magdalena, la hija del expresidente chileno, que sólo descargaba un troyano.
- Alerta de terremoto en Ecuador: un *email* prometía imágenes satelitales que sólo descargaban *malware*.
- ¡Michael Jackson está vivo!: el falso archivo sólo descargaba un troyano diseñado para convertir la computadora en un *zombi* que formará parte de una *botnet*.
- Romance entre Shakira y Alexis Sánchez: el falso video descargaba un troyano que modificaba los archivos *hosts* de la computadora afectada para hacer redirecciones.
- Ricardo Martinelli acusado de abuso: nuevamente un *email* prometía un falso video del presidente de Panamá que descargaba un troyano.

Por eso es importante que estés atento ante sucesos de esta masividad, y que tengas en cuenta que es muy probable que los cibercriminales los utilicen para tratar de engañar a los usuarios.

9.5 Proceso completo de como realizar un ataque de ingeniería social

Un ataque de ingeniería social inicia con una actividad de reconocimiento. Mientras más información se recolecte sobre la organización objetivo, mayores opciones se tienen disponibles. No es infrecuente iniciar con cero conocimiento y utilizar la información obtenida a través de fuentes abiertas para montar un simple ataque de ingeniería social; para obtener el directorio telefónico de la empresa, por ejemplo; y luego utilizar el nuevo conocimiento para montar un ataque de ingeniería social más selectivo y sofisticado, basado en la visión obtenida de la empresa.

Mientras el buscar en la basura es un ejemplo clásico de un punto de inicio con cero conocimiento para encontrar información sobre el objetivo, existen alternativas más convenientes. Google es probablemente la manera más efectiva de encontrar nombres, títulos de trabajo, información de contacto, y más. Una vez se obtenga una lista de nombres, se puede empezar a combinarlo con sitios de redes sociales como Facebook, LinkedIn y Twitter. Encontrar empleados con cuentas en los sitios populares de redes sociales es una práctica común entre los ingenieros sociales. Frecuentemente, estos empleados podrían estar conectados con otras personas con quienes trabajan. Dependiendo de los ajustes de seguridad, la red completa de conexiones podría ser visible, y se podría ser capaz de identificar a compañeros de trabajo fácilmente.

En el caso de sitios de redes para empresas como LinkedIn, la recolección de información es incluso más fácil, porque se puede buscar por el nombre de la empresa para encontrar empleados pasados y presentes del objetivo. En cualquier sitio de redes sociales, se puede también encontrar un grupo de ex empleados y empleados actuales de una empresa. Un blog específico y sitios de anuncios puede también producir información útil sobre temas de los empleados internos, los cuales están siendo discutidos actualmente. Frecuentemente estas publicaciones toman la forma de quejas anónimas, pero pueden ser útiles para demostrar un conocimiento interno cuando se entable conversación con el objetivo.

Utilizando métodos pasivos para recolectar tanta información sobre la empresa como sea posible, es un gran lugar para empezar a formular el ataque.

La ingeniería social es más exitosa como un esfuerzo de equipo, debido a la amplia variedad de circunstancias y oportunidades factibles de surgir. Como mínimo, dos personas podrían ser necesarios para los ejercicios más básicos. Mientras el carisma natural es un recurso preciado, una voz telefónica practicada y la capacidad de discutir convincentemente una amplia variedad de tópicos sociales no necesariamente técnicos, es ideal para avanzar en esta área. La capacidad de escribir convincentemente también es importante, como lo es la apariencia física para realizar ataques cara a cara o de suplantación. Como todas estas actividades son diseñadas para obtener acceso no autorizado hacia activos de datos, se debe también poseer conocimientos de Hacking, o al menos estar íntimamente familiarizado con sus posibilidades, para ayudar al equipo a tener una posición sobre la red y utilizarlo.

Un buen lugar para iniciar el reconocimiento después de buscar a la empresa en línea, es empezar a tener como objetivos a las personas internas de interés, en un intento por construir un cuadro de quien es quien y, si es posible, desarrollar una buena relación con potenciales fuentes. Personal clave podría incluir CIO, CSO, Director de TI, CFO, Director de Recursos Humanos, VPS, y directores de cualquier tipo. Todos estos individuos podrían tener buzón de voz, correo electrónico, secretarias, y similares. Conocer quien trabaja en cuales oficinas, quienes son sus asistentes personales, y cuando están de viaje o vacaciones podría no

parecer útil, pero lo es. Como ejemplo, si el objetivo es obtener el directorio interno de empleados. Conociendo cuando alguien está fuera de la oficina, se puede llamar a su asistente y clamar ser un consultor trabajando con su jefe, necesitando el directorio impreso del a empresa, y este sea enviado por fax hacia otra ubicación dentro de la empresa. En este punto, podría incluso preguntar si se requiere este sea enviado directamente a un correo electrónico, en cual caso el ataque de ingeniería social ha sido un éxito. Pero vamos a asumir no se consulta y se envía por fax directamente hacia otra oficina donde supuestamente se trabaja, se puede luego llamar a esta oficina dando una historia nuevamente, y preguntar si ha llegado un fax. Es factible también dar un número de fax público y obtener la información.

Este es un primer ejemplo de escalado de confianza. La primera victima no siente riesgo de enviar algo internamente. La segunda victima se siente confortable con el pretexto porque se ha demostrado conocimiento de las operaciones internas y no percibe ningún daño en pasar el directorio. Con el directorio en mano, se puede ahora utilizar un servicio para la falsificación de Identificadores de llamadas, para simular llamar desde el interior de la empresa. El siguiente movimiento es sencillo. Si la empresa, como la mayoría de empresas, es decir los IDs para los usuarios de red no son difíciles de inferir, se puede intentar vender un producto por teléfono para la gestión de identidad, o por ejemplo un juego de billar en el bar en el cual se conoce va, obtenida desde su permisiva página de Facebook. Se puede ahora llamar a soporte técnico desde el interior y tener el reseteo de la cuenta de alguien de recursos humanos de vacaciones, de tal manera se pueda utilizar la red privada virtual (VPN) remotamente.

Planear un ataque toma tiempo, práctica, y sobre todo paciencia. Debido al hecho de ser un atacante, se esta limitado únicamente por la imaginación. El éxito o falla dependerá de la capacidad del equipo para leer a la persona quien trabaja en la organización objetivo, y divisar un ataque o series de ataques de escalado, los cuales sean efectivos contra ellos. Se debe tener en mente, este es un juego de capturar la bandera. Algunas veces el objetivo es obtenido sin ninguna técnica tradicional de Hacking, utilizando métodos de acceso legítimo como credenciales concedidas erróneamente o robadas. En muchos casos, si embargo, esto es un esfuerzo combinado de tener un equipo de hackers en posición o entregar el “payload” o carga deseada de acceso remoto dentro de los controles del borde.

Así como los ataques se tornan más sofisticados, también se puede requerir configurar sitios webs, direcciones de correo electrónico, números de teléfono, con la intención de parecer una empresa legítima. Gracias a la proliferación de microempresas basadas en la web, y servicios de teléfonos móviles de pago, esto es ahora tan barato como trivial. Además de que también se puede también requerir reuniones cada a cara con la victima para ciertos tipos de ataques.

10. Ingenieros sociales notables

10.1 Kevin Mitnick

El delincuente informático reformado y posteriormente asesor de seguridad, Kevin Mitnick, señala que es mucho más fácil engañar a alguien para que facilite la contraseña de acceso a un sistema que esforzarse en intentar entrar en dicho sistema.

Kevin posiblemente haya sido una de las personas que haya llevado la ingeniería social a sus límites, que entre 1979 -con solo 16 años- y 1995 logró acceder a los sistemas de

empresas como Digital Equipment Corporation o Pacific Bell. Pero lo más llamativo de todo es que buena parte del trabajo no lo hizo desde un ordenador, lo hizo desde un teléfono.

Según explica en sus libros -El arte del engaño, El arte de la intrusión y El arte de la invisibilidad- hay cuatro aspectos compartidos por casi todas las personas que facilitan este trabajo:

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

Una de sus estrategias habituales era tras determinar quién era la persona que tenía la información que necesitaba. A continuación, se ponía en contacto con ella y llevaba la conversación a un punto donde él simulaba tener la información pero incorrecta, de forma que su interlocutor normalmente le corregía, dándole el dato que necesitaba.

10.2 Christopher Hadnagy

Es el profesional de seguridad que escribió el primer marco que define los principios físicos y psicológicos de la ingeniería social. Es más conocido por sus libros, podcast y por ser el creador de la DEF CON Social Engineer Capture the Flag y del Social Engineer CTF for Kids.

10.3 Mike Ridpath

Consultor de seguridad, autor y orador. Enfatiza técnicas y tácticas para la ingeniería social de "llamadas en frío" (cold calling). Se hizo notable después de dar charlas donde reproducía llamadas registradas y demostraba en vivo lo que hacía para conseguir contraseñas.

10.4 David Pacios

Creador del concepto Ingeniería Social Aplicada para distinguir casos de estafa digital y estudio del Hacking Social. Autor del libro *Ingeniería Social Aplicada: Primera línea de defensa* se hizo conocido por sus charlas y conferencias sobre hacking humano y comercio en *Deep Web*.

10.5 Badir Brothers

Los hermanos Ramy, Muzher, y Shadde Badir —todos ellos ciegos de nacimiento— lograron establecer un extenso esquema de fraudes telefónicos e informáticos en Israel en los años 90 utilizando ingeniería social, personificación de la voz y computadoras con pantalla Braille.

11. ¿Como puede afectar a las empresas y personas?

11.1 El 50% de las empresas víctimas de la ingeniería social

Según un estudio realizado por Check Point, proveedor de soluciones en seguridad de Internet, el 50 % de las empresas han sido víctimas de la ingeniería social. Los ciberdelincuentes habrían utilizado el phishing y las redes sociales para obtener información de la empresa. Los trabajadores recientemente contratados son los objetivos de los ciberdelincuentes.

Esta encuesta fue realizada en julio y agosto de 2011 por Check Point, se encuestó a más de 850 profesionales de informática y de seguridad en Estados Unidos, Canadá, Reino unido, Alemania, Australia y Nueva Zelanda.

Según los resultados del estudio, la ingeniería social, procedimiento para conseguir información relevante de la empresa por engaño o usurpación de identidad, sería un modo común de ataque dirigido a las empresas. Cerca del 48 % de las empresas interrogadas reconocen haber sido víctimas de este procedimiento cibercriminal, experimentando 25 o más ataques de la ingeniería social en los dos últimos años.

Los costos de estos ataques son particularmente elevados, cada ataque costaría entre 25 000 a más de 100 000 dólares según los profesionales que respondieron la encuesta. Los costos involucrarían: interrupción de la actividad empresarial, gastos de los clientes, pérdida de ingresos y el deterioro de la imagen de la empresa.

Otros resultados de este estudio:

- Los correos electrónicos de phishing, que buscan engañar y obtener la confianza del destinatario, representan la fuente más común de las técnicas de ingeniería social (47 %), seguidos de la información obtenida a través de las redes sociales, que contienen fuga de información personal y profesional, (39 %) y los terminales móviles mal asegurados (12 %).
- El afán de lucro es la razón más frecuente de los ataques de ingeniería social, seguida del deseo a acceder a información confidencial de la empresa (46 %), la búsqueda de ventajas competitivas (40 %) y los actos de venganza (14 %).
- Los nuevos trabajadores o colaboradores son los más vulnerables a las técnicas de ingeniería social.
- El 34 % de las empresas no han capacitado a los trabajadores en políticas de seguridad para evitar caer en los ataques de ingeniería social.

11.2 La importancia de tomar medidas e informar

En una charla TED, el Vicepresidente de Seguridad de IBM, Caleb Barlow, insta a las empresas de todo el mundo a combatir el cibercrimen de la misma manera que se llevan a cabo protocolos de actuación ante una crisis de salud mundial. Como hemos visto con los casos de la Gripe A o el virus del Zika, gobiernos y organismos de todo el mundo comparten

información al momento sobre la cantidad de personas afectadas y de cómo se está propagando el virus.

Este procedimiento es precisamente opuesto al que se lleva a cabo hoy en día en lo que respecta a los ataques informáticos. En comparación al número de ciberataques que se estima que se producen a diario, a penas se conocen datos de las compañías cuyos sistemas han sido vulnerados por miedo a que esto repercuta en su reputación, o incluso en sus resultados económicos. "Si no compartimos [información], entonces somos parte del problema" afirma Barlow.

12. Casos reales de ataques

12.1 Cuando blindar sistemas informáticos no lo es todo

En 2007 fue burlado uno de los sistemas de seguridad más caros del mundo. No hicieron falta armas, violencia, ni ningún tipo de aparato electrónico para que un hombre saliera con 28 millones de dólares en diamantes del banco ABM AMRO situado en Bélgica. El único arma que utilizó no se puede comprar: el encanto personal.

El tipo, que se hacía llamar Carlos Héctor Flomenbaum, tenía un pasaporte argentino que había sido robado en Israel. Con esta identidad se hizo cliente del banco y forjó la confianza de los empleados durante un año. Mientras se hacía pasar por un empresario de éxito, regalaba cajas de bombones a los trabajadores del banco. Un día, estos le dieron acceso a las cajas de seguridad que contenían gemas de 120.000 quilates, y entonces llevó a cabo uno de los mayores robos cometidos por una sola persona.

Con este ejemplo se saca en claro que el objetivo del robo eran las gemas, pero también refleja que el activo más importante de cualquier compañía sigue siendo la información. Posiblemente, el ladrón no hubiera sabido cosas como dónde se encontraban los diamantes si no hubiera sido porque los empleados le facilitaron estos datos. De ahí que las empresas no solo deban de invertir en sistemas de seguridad, sino en formar a cada uno de los miembros de su equipo por lo que pudiera pasar.

La moraleja es bien sencilla: no importa la tecnología de la que se dispone o cuán cara es esta, mientras intervenga el factor humano, el sistema sigue siendo vulnerable.

12.2 Caso Ubiquiti Networks

Ubiquiti Networks es un proveedor estadounidense de servicios de redes de alto rendimiento para empresas. En 2015 sufrió un ataque que le hizo perder 39.1 millones de dólares. Para ello, los cibercriminales escribieron algunos correos haciéndose pasar por miembros ejecutivos de la empresa, y pidieron a algunos empleados del área financiera que realizaran transferencias de grandes cantidades de dinero a una cuenta bancaria en particular. Como era de esperar, esta era propiedad de los cibercriminales.

Esta técnica de ingeniería social se aprovecha de ciertas debilidades del ser humano, como es el hecho de ser servicial, ya que eso podría incidir en el reconocimiento por parte de

los superiores. También se beneficia en que hay muchas personas que son incapaces de negarse a hacer algo que, pensado fríamente, podría resultar perjudicial.

Nadie se metió dentro de los sistemas informáticos de Ubiquiti Networks, tampoco robaron los datos de la compañía. En este caso, la brecha de seguridad estaba en los propios empleados, que carecían de la formación, y desconocían los procedimientos necesarios para protegerse ante este tipo de estafas.

12.3 La influencia de un falso tweet en la economía mundial

Hay quien lo habrá desterrado de su memoria, pero en abril 2013 la cuenta de Twitter de Associated Press publicó un tweet que durante unos minutos hizo tambalear la economía mundial:

Entonces, la red social no ofrecía a sus clientes el doble factor de autenticación para loguearse. Con lo cual, Syrian Electronic Army, el grupo que reivindicó la autoría del ataque, se hizo con la cuenta de Twitter a través del envío de un correo phishing a miembros del equipo de Associated Press. Alguno picó el anzuelo y facilitó las credenciales de acceso a los hackers. En la siguiente imagen se puede ver el correo phishing que fue enviado a Associated Press:

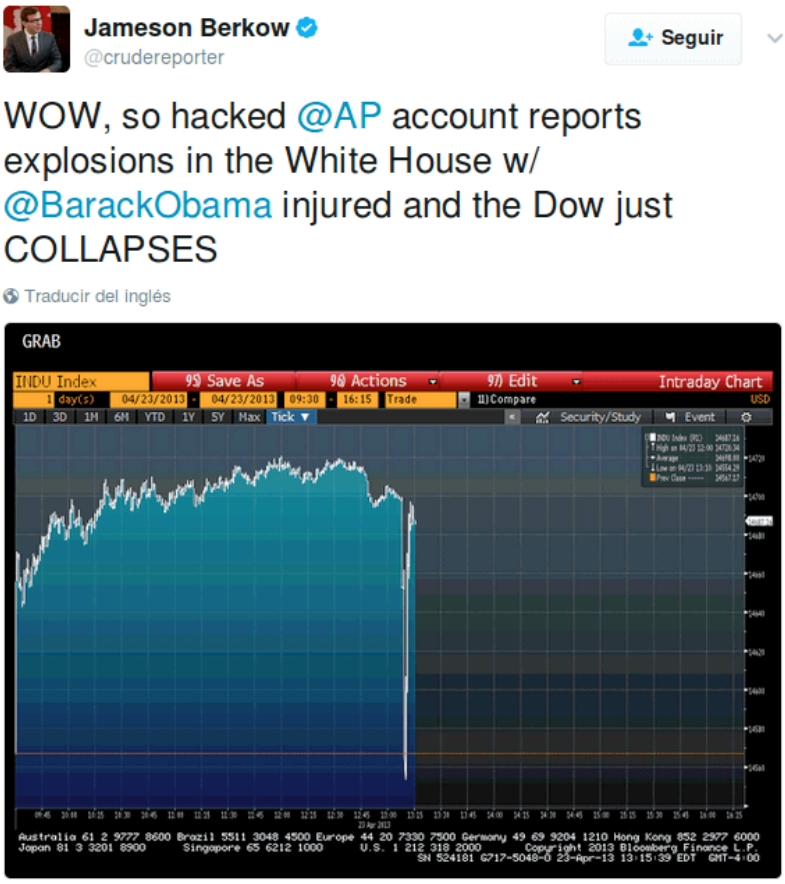
Hello,

Please read the following article, it's very important :

http://www.washingtonpost.com/blogs/worldviews/wp/2013/04/23/

[A different AP staffer]
Associated Press
San Diego
mobile [removed]

Hoy el desenlace es bien conocido: la Casa Blanca salió desmintiendo el tweet, y la cuenta de Associated Press fue temporalmente suspendida hasta que se recuperó su control. Los mercados también reestablecieron su orden.



Esta situación puso en evidencia lo frágiles que somos ante ciberataques de este tipo y, como consecuencia, lo vulnerables que son las compañías y organismos de cualquier nivel. Entonces fue Asocciated Press, pero mañana puede ser cualquier otra empresa o institución la que podría estar lanzando mensajes por sus redes sociales que perjudiquen su imagen, y por tanto, la confianza que tiene con sus clientes e inversores.

12.4 La estafa nigeriana (o estafa 419)

Es el cuento del tío de la era de Internet. ¿Quién no soñó con recibir una inesperada herencia de un pariente lejano?

Los estafadores detrás de este tristemente célebre engaño fueron precursores de algo que no solo perduró, sino que se expandió a diversos países e idiomas. Recibió su nombre a raíz del número de artículo del código penal de Nigeria que viola, ya que buena parte de las estafas provienen de ese país y de otros pertenecientes a África.

La estafa nigeriana promete a su víctima una gran fortuna, convenciéndola de que la suma le corresponde por una herencia, por ser ganador de un sorteo, por una generosa donación, porque las autoridades de un país lo necesitan o por otros diversos motivos. Como condición para acceder a ella, se exige el pago de un adelanto nada económico, pero bajo comparado con lo que supuestamente se va a ganar luego.

Naturalmente, existen numerosas variantes de la estafa nigeriana, como el que podemos ver en la siguiente captura:

Hello,

My name is Fernandez Flor, I am the branch manager of Banco [redacted] Quito Ecuador.
I have packaged a financial transaction that will benefit both of us, which
involves three million seven hundred and fifty thousand dollar $3,750.000.00.
Mean While you will have 35% of the total fund after the transaction.

If you accept this offer to work with me i will give you details on how we can
achieve it successfully. Please contact me with this email address:
fern[redacted]@blumail.org

Best Regards
Mr.Fernandez Flor

Oferta de $1.300.00 dólares al usuario si provee los datos de su cuenta

12.5 Estafas relacionadas a muertes de celebridades

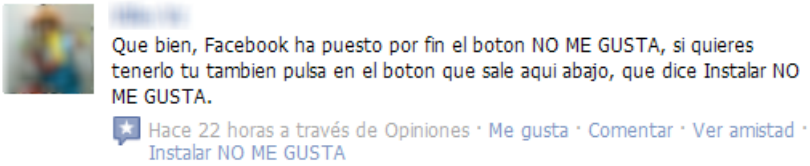
Los casos aquí abundan y no hacen más que demostrar cuánto les rinde a los cibercriminales aprovechar noticias de famosos fallecidos o incluso inventar que murieron, gracias a lo cual consiguen que cientos de usuarios curiosos hagan clic en enlaces engañosos.

Por mencionar algunos ejemplos, tenemos la falsa muerte del cantante Ricardo Arjona y también la del automovilista Michael Schumacher, el suicidio del actor Robin Williams o el rumor de que Michael Jackson estaba vivo.

12.6 Falsas noticias alarmantes de Facebook

Mucha gente cayó en el resonante engaño de que Facebook cambiaría su color a rosa, el cual se propagaba a través de mensajes en las biografías de los usuarios que contenían un

enlace. Al hacer clic, se producía una redirección a un sitio infectado. Algo similar sucedía con la supuesta posibilidad de ver quién visitó tu perfil, que a través del clickjacking obtenía al azar los nombres de los contactos de la víctima para publicar automáticamente en su muro y así continuar la propagación de la amenaza.

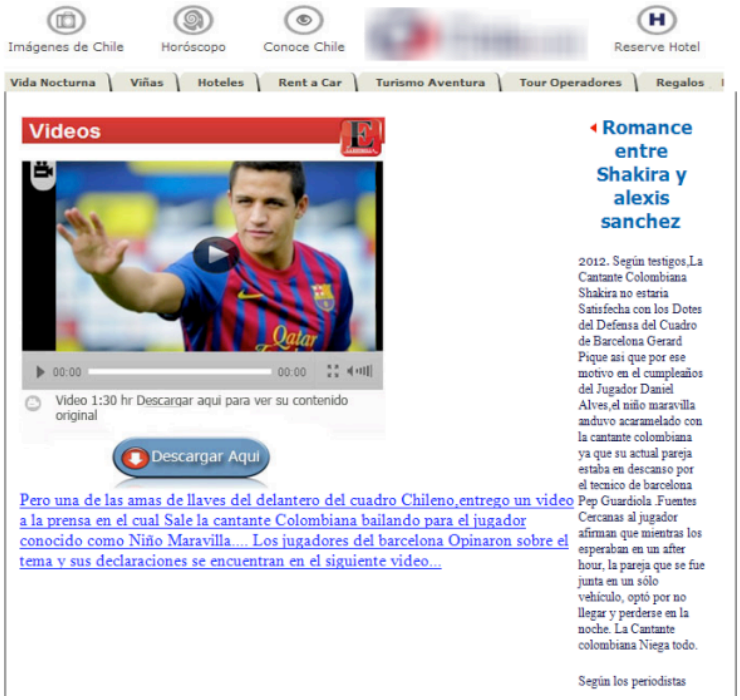


Igualmente famoso fue el falso botón "No Me Gusta", que terminaba ocasionándole a la víctima un gasto extra al quedar suscripta en servicios de SMS Premium. A fin de cuentas, en ese entonces Facebook nunca había anunciado la implementación de esta controversial característica.

12.7 Fotos y videos íntimos de famosos, para los más extremos

Muchas fueron las celebridades víctimas de la filtración de fotos íntimas, entre ellas Jennifer Lawrence, Ariana Grande, Rihanna, Kate Upton y Kim Kardashian, en lo que se conoció como *Celebgate*. Como consecuencia, no tardaron en aparecer amenazas disfrazadas de archivos y carpetas conteniendo el material robado, así como estafas con enlaces que supuestamente permitían ver videos XXX de las actrices.

También Shakira fue objeto de una campaña que propagaba en Facebook un falso video íntimo, en el que la cantante supuestamente había cometido en público un acto poco digno. Al poco tiempo, apareció otro supuesto video que aparentaba mostrar un romance oculto entre ella y el jugador de fútbol Alexis Sánchez, basado en el hecho de que su pareja real**,** Gerard Piqué, no tenía tantos dotes como ella hubiera querido.



12.8 WhatsApp para PC, estafa antes de realidad

WhatsApp Web ya está ampliamente adoptado en la comunidad de usuarios móviles, pero antes, cuando todavía no existía este programa en forma legítima, era un frecuente gancho de estafas. Como millones de personas lo esperaban, eran muchos los que hacían clic sin dudarlo cuando se encontraban con una oferta de WhatsApp para PC.

From: WhatsApp para PC <whatsapp@microlink1.com.br>
To:
Subject: Novo WhatsApp para Windows
Date: 2014-01-07 07:10:10

WhatsApp
Agora também para PC!

Use o WhatsApp agora também no seu computador

Você já teve vontade de poder usar o WhatsApp também no seu computador e não sabia como? Agora o WhatsApp também pode ser usado no seu PC de forma idêntica ao do seu celular, e o melhor, totalmente grátis. Sem ter que pagar anuidade.

Baixe e teste agora mesmo

Download

Ese es precisamente el título que llevaba un engaño, que contenía un malware enfocado en la extracción de información personal bancaria.

13. Conclusiones

La ingeniería social es una técnica que es difícil de identificar cuando se esta aplicando, por lo que es vital, para la protección informática, que se establezcan mecanismos y procedimientos para prevenirla. Sin embargo, se podrá contar con los mecanismos más avanzados y los procedimientos mejor estructurados, pero si el usuario hace caso omiso de los mismos, de nada habrán servido.

La herramienta más eficiente con la que cuentan las organizaciones para contrarrestar la ingeniería social es la concientización, es decir, que el usuario identifique la importancia de la actividad que realiza, del valor de la información que maneja y el buen uso que debe llevar a cabo sobre el hardware y software que se encuentran bajo su responsabilidad.

Es importantísimo hacerle saber al usuario que es él, precisamente, el eslabón más débil en la cadena de usuarios de un sistema informático, debido a que en él impactan distintos factores que influyen en la conducta humana, como pueden ser la confianza en otras personas y el desinterés en lo que esta realizando; factores que se convierten en oportunidades de ataques a los activos informáticos.

Finalmente se han logrado los objetivos propuestos de dar un punto de información unificado para adentrarse en el ámbito de la ingeniería social y todo lo que le rodea. Aunque se hayan tenido que mover algunos puntos a desarrollar del orden inicial por coherencia del contenido, y eliminado alguno por falta de información del mismo. Por lo que a groso modo se ha cumplido con la planificación inicial.

14. Bibliografía

- https://www.pabloyglesias.com/mundohacker-ingenieria-social/
- http://www.1000tipsinformaticos.com/2017/03/que-es-la-ingenieria-social-tipos-de-ataques.html
- https://opendatasecurity.io/es/ingenieria-social-cuando-blindar-sistemas-informaticos-no-lo-es-todo/
- http://www.reydes.com/d/?q=Realizar_un_Ataque_de_Ingenieria_Social
- https://underc0de.org/foro/hacking/la-ingenieria-social/
- https://mywebsecurity.wordpress.com/ingenieria-social/
- https://www.elespanol.com/social/20170704/228727707_0.html
- http://tecnologiapunta.net/ingenieria-social-y-seguridad-informatica/
- https://www.azulweb.net/la-ingenieria-social-algunas-formas-llevarla-cabo/
- http://es.ccm.net/contents/25-ingenieria-social
- http://es.ccm.net/faq/7695-el-50-de-las-empresas-victimas-de-la-ingenieria-social
- https://www.fwhibbit.es/ingenieria-social-iv-asumiendo-roles-en-distintos-escenarios
- https://underc0de.org/hacking/ingenieria-social.html
- https://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/
- http://www.conasa.es/blog/seguridad/ingenieria-social-el-arte-de-obtener-informacion-confidencial/
- https://espanol.totalbank.com/seguridad/todo-lo-que-debe-saber-sobre-la--ingenieria-social-
- http://www.proteccionononline.com/%C2%BFque-es-la-ingenieria-social-en-que-consiste-y-como-evitar/
- http://www.magazcitum.com.mx/?p=2747#.Ww2wVam-lTY
- https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)
- http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO74-2011.IngenieriaSocial_LuisdeSalvador.pdf
- http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/
- https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana
- https://es.ccm.net/contents/25-ingenieria-social
- https://www.incopyme.com/ingenieria-social/
- https://www.pandasecurity.com/spain/mediacenter/seguridad/ingenieria-social-empresas/
- http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/
- http://www.eltiempo.com/opinion/columnistas/guillermo-santos-calderon/ojo-a-la-ingenieria-social-que-afecta-a-las-personas-217088
- https://blog.seur.com/ingenieria-social-que-es/
- https://omega2001.es/ingenieria-social/
- https://www.welivesecurity.com/la-es/2015/12/01/historias-de-ingenieria-social-ridiculas/