Estudio de Metodologías de Ingeniería Social

Alejandro Méndez Carvajal
Máster Universitario En Seguridad De Las Tecnologías De La Información Y De Las Comunicaciones (MISTIC)
TFM – Ad hoc

Director de TFM: **Ángela María García Valdez**
Docente responsable asignatura: **Víctor García Font**

Diciembre 2018

Agradecimientos

A mi Padre Celestial, por el entendimiento y descernimiento en el cumplimiento de los logros y objetivos, establecidos en el programa del Máster.

A mi esposa Francy, compañera de vida y de logros, por el amor, apoyo y su comprensión en el tiempo dedicado en esta etapa de formación profesional.

A mi madre Luz Marina, por sus oraciones, bendiciones y amor incondicional.

A la UOC, tutores, docentes y compañeros de estudio, por su apoyo, enseñanzas, retroalimentación y conocimiento compartido.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Estudio de Metodologías de Ingeniería Social*
Nombre del autor:	*Alejandro Méndez Carvajal*
Nombre del consultor/a:	*Ángela María García Valdez*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega:	12/2018
Titulación:	Máster Universitario En Seguridad De Las Tecnologías De La Información Y De Las Comunicaciones (MISTIC)
Área del Trabajo Final:	*TFM – Sistemas de Autenticación y Autorización*
Idioma del trabajo:	*Español*
Palabras clave	*Metodologías Ingeniería Social*

Resumen del Trabajo:

El trabajo presenta un estudio sobre las diferentes metodologías de Ingeniería Social que están utilizando los delincuentes, para llevar a cabo fraudes con la información que obtienen de sus víctimas sin que ellas se percaten.

Para lo cual, se brindan las recomendaciones para prevenir las personas, fortalecer el sentido común y mitigar el riesgo de no ser víctima del robo de información.

Se realiza una introducción sobre el concepto de ingeniería social, los roles que intervienen, el tipo de información que se puede obtener, cómo se obtiene provecho de la misma y las leyes a nivel mundial que persiguen estas actuaciones de los delincuentes.

Lo anterior, hace parte la gestión que llevo a cabo como CISO a nivel profesional y con las personas de mi entorno. Es mi propósito, que este trabajo final de máster, sea conocido por muchas más personas, para que sean sensibilizados sobre el riesgo al que todos estamos expuestos y sigan las recomendaciones para que cada vez, sean menos los eslabones débiles de la cadena.

Abstract:

The work presents a study on the different Social Engineering methodologies that criminals are using, to carry out frauds with the information they obtain from their victims without them noticing.

To this end, recommendations are provided to prevent people, strengthen

common sense and mitigate the risk of not being a victim of information theft.

An introduction is made about the concept of social engineering, the roles that are involved, the type of information that can be obtained, how it is obtained and the laws worldwide that pursue these actions of the criminals.

The above is part of the management that I carry out as a CISO at a professional level and with the people around me. It is my purpose that this final master's project is known by many more people, so that they are aware of the risk to which we are all exposed and follow the recommendations so that each time, there are fewer weak links in the chain.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

Las mayores brechas de seguridad de la información hoy en día, no son los virus informáticos que generan fuga o pérdida de información en los sistemas informáticos, son las diferentes metodologías de ingeniería social que utilizan los delincuentes para obtener información de forma no autorizada. Por lo anterior, se formula el problema a resolver: ¿Qué hábitos de seguridad, se deben fomentar en las personas en su cotidianidad y vida laboral, para disminuir los ataques de ingeniería social?

1.2 Objetivos del Trabajo

Este documento, presenta un estudio de las metodologías de la ingeniería social y las técnicas que son implementadas, para lograr obtener información.

Se brinda al lector el significado y conceptos para lograr el entendimiento de la ingeniería social, las diferentes formas en las cuales se obtiene la información y cómo fortalecer el sentido común y mitigar el riesgo de no ser víctima del robo de información.

1.3 Enfoque y método seguido

Se llevó a cabo un estudio de las diferentes técnicas actuales de ingeniería social, a través de recursos web, audiovisuales y libros, a través de 4 fases y aspectos que enmarcan una investigación cualquiera y que permiten obtener un resultado óptimo y adecuado.

1.4 Planificación del Trabajo

A través de un diagrama de Gantt, se ha gestionado la planificación temporal detallada de las tareas y dependencias del Trabajo Final de Master (TFM).

Nombre de tarea	Duración	Comienzo	Fin
TFM	**88 días**	**mié 19/09/18**	**vie 18/01/19**
Inicio del proyecto	**1 día**	**mié 19/09/18**	**mié 19/09/18**
PEC1	**13 días**	**jue 20/09/18**	**lun 8/10/18**
PEC2	**20 días**	**mar 9/10/18**	**lun 5/11/18**
PEC3	**20 días**	**mar 6/11/18**	**lun 3/12/18**
PEC4 Memorial Final	**1 día**	**lun 31/12/18**	**lun 31/12/18**
Presentación / Video	1 día	lun 7/01/19	lun 7/01/19
Defensa del TFM	1 día	vie 18/01/19	vie 18/01/19

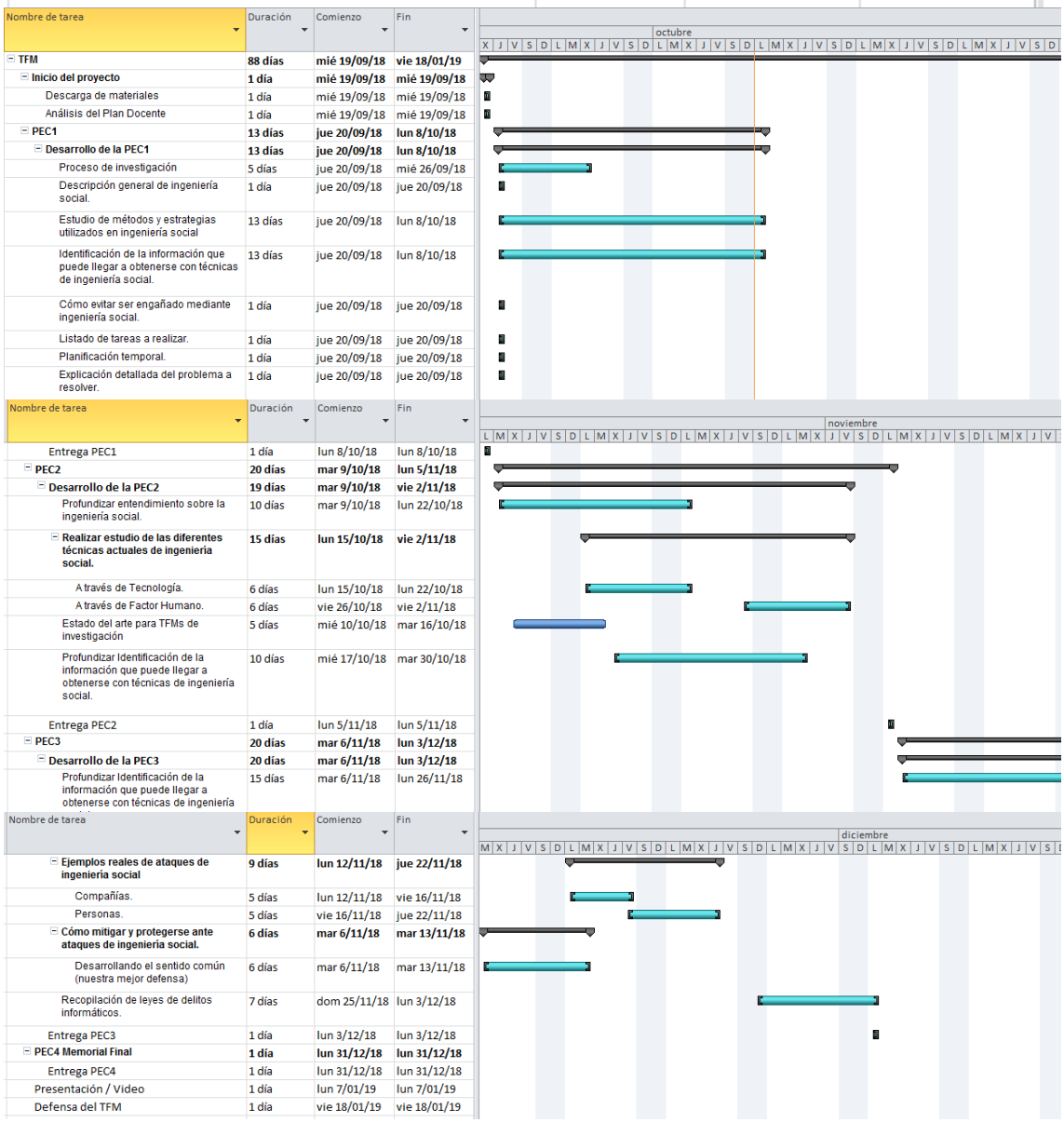


Ilustración 1: Planificación TFM.

1.5 Breve sumario de productos obtenidos

A continuación, se relacionan los diferentes puntos desarrollados:

- Introducción
- Descripción de ingeniería social: ¿Qué es la ingeniería social?
- ¿Cómo podemos estar protegidos y mitigar el riesgo de ser víctimas de la ingeniería social?
- ¿Qué roles intervienen en la ingeniería social y cuáles son sus características?
- Métodos y estrategias en la ingeniería social
- ¿Qué información puede llegar a obtenerse con éstas técnicas y cómo los cibercriminales la explotan para obtener beneficios?
- Ataques de ingeniería social más comunes
- ¿Cómo poder evitar ser engañado mediante ingeniería social?
- Leyes a nivel mundial para perseguir las actuaciones de la ingeniería social.
- Conclusiones
- Glosario

2. Descripción de ingeniería social: ¿Qué es la ingeniería social?

Se puede afirmar que la ingeniería social es una técnica basada en el engaño y busca sacar provecho de las debilidades que ostentan las personas, ajustable en cualquier momento de la cotidianidad o vida laboral. Es decir, es la capacidad para influenciar en la conducta y toma de decisiones de los seres humanos. La ingeniería social presenta dos vectores principales de ataque:

- *Basados en el uso de tecnología*, haciéndole creer a las personas que están interactuando verdaderamente con un programa o sistema de información, con el propósito de obtener información privilegiada.

- *Basados en el engaño humano,* utilizando la naturaleza humana de ser útil, eficiente, congraciar o caer muy bien para acceder a información valiosa.

Según opinión de Kevin Mitnick: “usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, controles de acceso, etc. Lo único que se necesita, es un llamado a un empleado desprevenido e ingresar sin más. Tienen todo en sus manos”, de igual forma, afirma que la ingeniería social se basa en estos cuatro principios:

- 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.

De acuerdo con Christopher Hadnagy, en el libro Social Engineering: The Art of Human Hacking (Ingeniería Social: El Arte del Hacking Personal), define la ingeniería social como: “el acto de manipular a una persona para que tome una acción que puede, o no, ser objeto de su interés. Esto puede incluir la obtención de información, acceso, o consecución de un objetivo en específico”.

Con un detalle más profundo, Christopher Hadnagy, en su libro Unmasking the Social Engineer: The Human Element of Security (Desenmascarando al Ingeniero Social: El Elemento Humano de la Seguridad). Relaciona la ciencia de la comunicación no verbal con el arte de la ingeniería social, donde coincide con la mayoría de los investigadores, en que gran parte de lo que comunicamos, no se hace a través de lo que decimos, sino de cómo se dice. Una combinación de nuestras expresiones faciales, lenguaje corporal, tono vocal y otros indicadores puede indicar al receptor nuestra intención, nuestro contenido emocional y el significado detrás del mensaje. Las personas sin ser conscientes, deciden confiar en alguien con base en su postura, sonrisa y lenguaje corporal o se sienten incomodos con alguien, por la falta de una sonrisa o lenguaje corporal agresivo.

3. ¿Cómo podemos estar protegidos y mitigar el riesgo de ser víctimas de la ingeniería social?

La mejor manera es a través de la educación continua. Todos los empleados que hacen parte de una Compañía, desde el personal de servicios generales, personal administrativo, operaciones, tecnología y alta gerencia, deben estar capacitados en cuanto a las debilidades y los métodos de engaño más comunes empleados por los delincuentes, para que puedan identificarlos e informar sobre cualquier anomalía.

Este proceso de formación y de concienciación, por parte de las Compañías hacia sus clientes internos y externos, debe estar incluido dentro del proceso de capacitación, para generar una cultura de seguridad de la información y que, a la vez, esté en constante dinámica, previendo los posibles cambios a futuro.

Definitivamente con la educación desde nuestros hogares y formación continua por iniciativa propia, mitigarían en gran manera los riesgos de afectación en lo que a ingeniería social se refiere. Es un largo camino por recorrer y que, junto a la continua evolución de las tecnologías, será cada vez más extenso. En el capítulo 8, se brindarán las recomendaciones para evitar ser víctimas de la ingeniería social.

4. ¿Qué roles intervienen en la ingeniería social y cuáles son sus características?

Antes de llevar a cabo la validación de los roles y características que intervienen en la seguridad de la información, es importante hacer aclaraciones para tener un mayor contexto sobre términos que hoy en día, son utilizados con mayor frecuencia, en el ámbito de la seguridad informática. A continuación, se relacionan las siguientes definiciones:

- Crackers: También conocidos como Black hat (Sombrero Negro) reflejan sus habilidades en informática, vulnerando la seguridad de sistemas de información, colapsando servidores, entrando a zonas restringidas, infectando redes o apoderándose de ellas, a través de sus destrezas en métodos de hacking.

- Defacer: Buscan bugs de páginas web, con el propósito de infiltrarse en ellas y así modificarlas.

- Ethical hackers/Pentesters: También conocidos como White hat (Sombrero Blanco) reflejan sus habilidades en informática vulnerando la seguridad de sistemas de información, sin colapsar servidores, entrando a zonas restringidas, sin infectar redes, a través de sus destrezas en métodos de hacking, con el propósito de evidenciarlos y gestionar los controles que mitiguen las brechas de seguridad evidenciadas.

- Hackers: Gente apasionada por la seguridad informática. Este término es utilizado para describir a alguien que "hackea" un sistema de información por medio de redes de comunicación, con el objetivo de eludir o desactivar las medidas de seguridad, si lo hace de forma no autorizada es conocido como Black hat (Sombrero Negro). Pero también, incluye a aquellos que depuran y arreglan errores en los sistemas White hat (Sombrero Blanco) y a los de doble moral como son los Grey hat (Sombrero Gris).

- Hacktivistas: Es una perspectiva más amplia del hacker, pero con una orientación a su integración al hacktivismo en tanto movimiento. En este sentido los hacktivistas son parte de una conciencia colectiva que promueve la libertad del conocimiento, la justicia social, creando nuevos sistemas, herramientas y aplicaciones tecnológicas para ponerlas a disposición del dominio público.

- Lammer o script-kiddies: Son aprendices que presumen ser lo que no son, aprovechando los conocimientos del hacker y poniéndolos en práctica, sin saber a ciencia cierta los mismos. No saben nada de hacking o utilizan programas de hackers, indicando que fueron generados por ellos. Más de alguna vez terminan comprometiendo sus propios equipos de cómputo.

- Newbie: Es un término utilizado para describir a un novato, es el que no posee muchos conocimientos en hacking.

- Pharmer: Se dedican a realizar ataques de tipo “phishing”, donde el usuario cree que está entrando a un sitio real y en realidad introduce sus datos en uno creado por el cracker.

- Phreaker: Esta palabra proviene de Phone Freak (monstruo telefónico). Son personas con conocimientos en teléfonos modulares y móviles, se encuentran sumergidos en entendimientos de telecomunicaciones bastante amplios. Generalmente Phreakers, son aquellos a los que les interesa el tema de hacking, pero que por estar empezando no son reconocidos por la elite.

- Programador Vodoo: Es el programador que se basa en técnicas que leyó, pero que todavía no entiende. Así que las mismas podrían funcionar o no.

- Samurái: Comúnmente son contratados para investigar fallos de seguridad informática, investigan casos de derechos de privacidad, amparados en regulaciones y leyes. Los samuráis persiguen a los crackers y a todo tipo de criminales informáticos. En medio de su gestión, dedican tiempo en concientizar sobre la seguridad informática.

- Sneaker: Personas contratados para romper los sistemas de seguridad por las empresas e instituciones, con la intención de subsanar dichos errores.

- War driver: Son crackers que saben aprovechar las vulnerabilidades de todo tipo de redes de conexión móvil.

- Wizard: Es el que conoce a detalle cómo actúa cada sistema de información por complejo que sea. Un hacker usa técnicas avanzadas, pero el wizard entiende cómo o por qué funcionan, facilitando su interacción y conociendo las brechas de seguridad.

Después de haber validado la terminología mencionada anteriormente, es importante, tener presente que, en la ingeniería social se suelen tomar varios roles con el objetivo de lograr llevar a cabo una infiltración o pasar desapercibido.

Es sabido por muchos, que un ingeniero social es un muy buen actor y para lograr sus objetivos, debe prepararse muy bien, realizando un reconocimiento del escenario donde actuará, recolectando información tanto virtual como física, para adaptar la expresión corporal y verbal requerida, luego, relacionando esta información para establecer

correlación y finalmente, usándola para llevar a cabo el ataque y obtener o llegar a su objetivo.

Por otro lado, las personas que desempeñan sus roles en la vida laboral aplican ingeniería social muchas veces, sin ser conscientes de ello, por ejemplo: en el ámbito de los gobiernos, el rol que asumen los políticos al hacer uso de su poder para controlar diferentes situaciones, creando distracciones, con el propósito de desviar investigaciones o generar controversias en la oposición y en la misma sociedad. Lo anterior, lo logran llevando a cabo discursos carismáticos, asertivos y conociendo las necesidades de las personas, prometen hasta lo imposible, donde al final decepcionan a todos, eso sí, después de lograr su cometido.

Otro caso, es el de los médicos y terapeutas, que convencen a sus pacientes de consumir un medicamento o tratamiento en pro de su salud, muchas veces sin que, el mismo, conlleve a obtener resultados positivos. Y un rol más simple, como el de un niño que manipula a sus padres, en el mayor de los casos, a través de un berrinche o pataleta para obtener lo que quiere.

5. Métodos y estrategias en la ingeniería social

A continuación, se relacionan, diferentes métodos y estrategias utilizadas en la ingeniería social, que pretenden sacar provecho de características de los seres humanos, como lo son: miedo, halago, necesidad, ayuda, deseo y codicia, con el fin de lograr obtener información sensible accediendo a sistemas de información de forma no autorizada.

- Affectivity (Afectividad): Es la susceptibilidad que tienen las personas ante situaciones específicas en su entorno, lo que es aprovechado por los ingenieros sociales para conseguir su objetivo.

- Baiting: Es una técnica muy efectiva, que utiliza pendrives con software malicioso, los que dejan en lugares de acceso concurrido de la víctima para que los encuentre y los conecte en sus equipos de cómputo.

- Carding: Inicialmente se basaba en robar tarjetas de crédito que podían ser usadas para realizar compras ilegales hasta que fueron canceladas. No obstante, hoy en día, el principal método usado para robar la información de la tarjeta de crédito, datos financieros u otros detalles sensibles, están relacionados con el malware o phishing.

- Correos electrónicos con malware: Los correos electrónicos pueden traer adjuntos cualquier tipo de archivos, contenedores de alguna clase de malware, como: virus, gusanos, troyanos,

Rootkits, ransomware, entre otros; cada uno, con una tarea específica y características especiales. Cuando la víctima los abre o descarga, se presenta la infección del equipo de cómputo.

- Deceptive Relationships (Relaciones basadas en engaños): Lo que se busca es crear relaciones personales para lograr conseguir información.

- Dumpster Diving / Trashing (Buscar en la basura): Los ingenieros sociales pueden encontrar en las sestas de basura todo tipo de información, tanto física como electrónica, datos financieros, recibos de servicios públicos, post-it con credenciales, en general, información sensible de negocio.

- Escuchar detrás de las Puertas: Es como lo menciona su nombre, donde también incluye escuchar conversaciones sin autorización, en lugares públicos u oficinas, apoyándose muchas veces de dispositivos tecnológicos.

- Googling: Es simplemente hacer uso de uno de los buscadores más reconocidos y mejor posicionados: Google. Lo anterior, debido que casi toda la información del mundo, se encuentra en el ciberespacio y por suerte para los ingenieros sociales, gran parte de empresas y la gran mayoría de personas, no aplican los controles de privacidad requeridos, en el manejo de su información en la nube.

- Grooming (Acicalar): Se utiliza para hacer referencia, a todas las conductas o acciones, que realiza un adulto para ganarse la confianza de un menor de edad, con el objetivo de obtener beneficios sexuales.

- Hoax (Trampa o Broma): Se presenta en cadenas de correo electrónico, que circulan con mensajes falsos sobre pedidos de ayuda ante una persona que padece una enfermedad, o bien, frente a textos que advierten premios, sí reenviamos el correo en cuestión a nuestros contactos.

- Office Snooping: Es el acceso no autorizado a los datos de otra persona o Compañía. Muy similar al escuchar detrás de las puertas, pero no se limita necesariamente a obtener acceso a los datos durante su transmisión. Puede incluir la observación casual de un correo electrónico, que aparece en la pantalla de la computadora de otra persona o ver lo que otra persona está escribiendo.

- Overloading (Sobrecarga): Se basa en hostigar a la víctima con gran cantidad de información en un corto periodo de tiempo, a tal punto, que se sienta confundida, logrando que ésta acceda, a las razones o demostraciones del ingeniero social.

- Phishing: Son mensajes de correo electrónico, SMS o comunicados por redes sociales en los cuales piden ingresar a través de un link a una página web (falsa). Los criminales copian la totalidad de una página real y la publican en servidores que presentan vulnerabilidades, estos servidores son de personas ajenas a la entidad y al delincuente, donde se solicitan datos y claves personales, para efectos de actualización de información, blindaje de IP, actualización tecnológica, compras no autorizadas, fraudes, entre otros.

- Pop–ups: Son ventanas emergentes que despliegan algunos sitios web o aplicaciones con el fin de presentar o mostrar algún tipo de información al usuario. Pueden ser una fuente malware, crear ciclos o bucles infinitos de apertura de ventanas, afectando la interacción del usuario con el equipo de cómputo.

- Pretexting / Impersonate (Pretender / Personificar): Estas técnicas van de la mano y pueden usarse tanto en los ataques locales, como en los remotos. Se presenta cuando el atacante se hace pasar por un empleado de TI. Trata de generar empatía para ganar credibilidad con su víctima, presenta algún tipo de excusa o pretexto, como alertar a la víctima de un comportamiento inadecuado en su equipo de cómputo. De esta manera, brindará pasos a seguir, para que instale un malware o le permita acceso remoto.

- Reciprocity (Reciprocidad): Las personas tienden a sentirse comprometidos cuando otro presta su ayuda. Quien la recibe, espera dar algo a cambio como ejemplo de gratitud. Así, un ingeniero social resuelve un problema sin interés alguno, y de esta forma, la victima siente la necesidad de responder de la misma forma.

- Reverse Social Engineering (Ingeniería Social Inversa o técnica de las migas de pan): Se presenta cuando un hacker causa problemas en la red objetivo o equipo de cómputo, provocando que el mismo vaya a solucionar el problema. Una vez ha solucionado el problema, adquiere la confianza del dueño de la información para llevar a cabo su protervo propósito.

- Shoulder Surfing (Espiar por encima del hombro): Es una de las modalidades más comunes. Normalmente se evidencia en las filas de los bancos o cajeros electrónicos, consiguiendo ver las claves de sus víctimas o en sitios públicos como un café internet, donde se logra ver lo que digita la otra persona; en ocasiones se emplean dispositivos de grabación electrónica para captar de una mejor forma la información.

- Scam (Timo o Estafa): Su objetivo con la víctima es llevarla a una historia o situación, en la que se dice que uno o varios individuos entregan una cantidad de dinero al estafador o "Scamer" con la promesa de recibir a cambio un beneficio generalmente económico.

- Sexting: Hace referencia al envío y/o recepción de contenido sexual a través de medios electrónicos. El mismo, consiste en el intercambio de imágenes y vídeos sexuales a través de chats, redes sociales o e-mail utilizando dispositivos móviles en su gran mayoría.

- Sextorsión: Es una forma de extorsión en la que se busca chantajear a una persona, por medio de una imagen o vídeo de sí misma comprometedor (desnuda), que pudo haber compartido a través de Internet o chat. La víctima es coaccionada a cancelar sumas de dinero, para no divulgar la información en la web y entorno social o ejecutar acciones que den gratificación sexual al delincuente.

- Spam (correo basura): También conocido como correo no deseado o no solicitado, enviado por "spammers", cuyo objetivo es lograr el "colapso servidores y sobrecarga de buzones de correo". Normalmente son correos con publicidad, no obstante, es posible que contengan malware o phishing.

- Suplantación de identidad: El ingeniero social asume un rol que represente autoridad o necesidad, por ejemplo: puede hacerse pasar, en una llamada telefónica, por un usuario legítimo y contactarse con el departamento de TI, para que le cambien su contraseña o caso contrario, hacerse pasar por personal de TI, indicando a un usuario legítimo que requiere de sus credenciales, para solucionar un problema en el sistema que está causando el mismo usuario. También, puede pretender tener un cargo directivo y requerir información sensible por teléfono o correo electrónico.

- Tailgating / Piggybacking: (Obtener acceso físico): Este tipo de ataque se aprovecha de la solidaridad y buena voluntad de las personas. Suele presentarse cuando un empleado (víctima) está ingresando a su empresa, la cual posee algún tipo de restricción en su acceso físico y el atacante con un gesto de torpeza porque olvidó sus credenciales, solicita ayuda para poder ingresar.

- Vishing: Es la modalidad en la cual el ingeniero social, a través de una llamada, busca llamar la atención de su víctima para obtener información sensible. Un ejemplo, es cuando llaman a un tarjeta-habiente indicándole que están haciendo compras con sus TC y que, para detener la transacción, debe informar el número de su

TC, fecha de vencimiento y CVV (código al respaldo de las TC para autorizar compras).

6. ¿Qué información puede llegar a obtenerse con éstas técnicas y cómo los cibercriminales la explotan para obtener beneficios?

Cuando un cibercriminal lleva a cabo técnicas de explotación de ingeniería social, busca obtener:

En Compañías:

- Estrategias de negocio.
- Credenciales o contraseñas.
- Perfiles de usuarios con acceso a los sistemas de información.
- Información confidencial.
- Recursos de sistemas.
- Estados financieros aún no públicos.
- Bases de datos de clientes (datos personales y/o financieros).

En Personas:

- Datos personales:
  - ID/DNI.
  - Estado civil.
  - Correo electrónico personal y corporativo.
  - Teléfono/Celular personal y corporativo.
  - Dirección de correspondencia personal y corporativa.
  - Creencias.
  - Tendencia sexual.
  - Historia clínica.
  - Cargo cómo empleado.
  - Salario.
- Contraseñas.
- Perfiles de usuarios en redes sociales.
- Información financiera
  - Números de productos financieros.
- Credenciales de juegos online.

Los cibercriminales utilizan la información obtenida para:

- Chantajear.
- Perfilar malware.
- Venderla a la competencia.
- Generar documentación falsa.
- Extorsionar (por teléfono, email, SMS, redes sociales).
- Generar nuevos vectores de ataques y obtener más información.

- Venderla en la deepweb o darkweb. A continuación, se relaciona imagen con la lista de precios de cibercrimen:

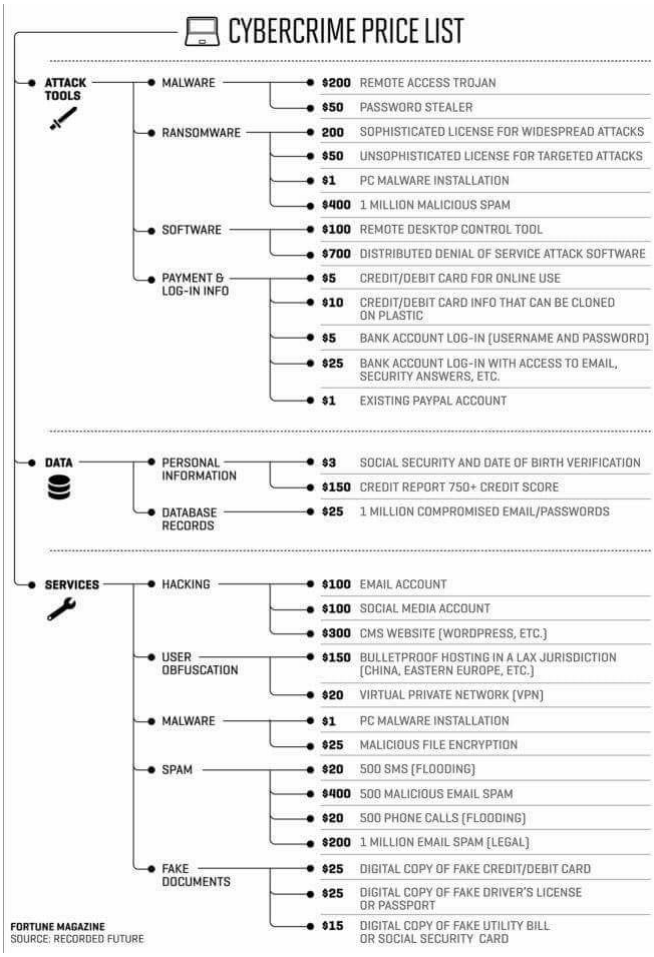


Ilustración 2: Precios de lista de cibercrimen.

7. Ataques de ingeniería social más comunes

A continuación, se relaciona la forma en la que se ejecutan varios los ataques de ingeniería social:

En Compañías:

- Llamada de la Mesa de Ayuda: Los delincuentes se hacen pasar por personal de soporte, para contactar a un usuario y obtener información, usualmente de credenciales de acceso. Lo anterior, se puede presentar en dos escenarios:

  - Primer escenario:

    - Delincuente: Buenos días, le llamo del departamento de tecnología.

- Víctima: Buenos días.

- Delincuente: Notamos un comportamiento extraño generado desde su equipo en la red.

- Víctima: ¿Cómo así?

- Delincuente: Si señor@, en estos momentos identificamos que su equipo está generando mucho tráfico y nos es imposible identificar que está generando este extraño comportamiento. Debo solicitarle su colaboración indicándome el usuario con el que inicia sesión y la contraseña ya que debo realizar una conexión al mismo y validar si hay algún virus o software malicioso afectando la red.

- Víctima: claro que sí.

- Delincuente: Permítame realizo una prueba de conexión, no será necesario que deje de trabajar.
  Si señor@, acabo de identificar que su equipo cuenta con un problema, en un momento nos acercaremos a revisar su equipo.
  Muchas gracias por su colaboración.

- Segundo escenario:

  - Delincuente: Buenos días, le llamo del departamento de tecnología, de acuerdo con un aviso que me está generando el servidor noto que su cuenta de SAP está generando un fallo en varios módulos.

  - Víctima: Buenos días.

  - Delincuente: ¿Me podría indicar que operaciones ha realizado en la mañana/tarde del día de hoy?

  - Víctima: - 'Procede a dar detalle de lo realizado'.

  - Delincuente: Entiendo, si, no debería presentarse problema alguno con esas transacciones.
    ¿Me podría recordar su usuario de SAP para realizar una validación en el servidor?

  - Delincuente: Si, evidencio que hay algunas fallas con su cuenta, debo solicitarle su colaboración, me podría facilitar su contraseña de acceso a SAP para replicar el fallo en mi equipo y solucionar el problema.

  - Víctima: Sí, claro le confirmo los datos.

- Delincuente: Bueno, realizaremos las revisiones y en el transcurso del día me comunicaré de nuevo para indicarle que ha pasado.
  Muchas gracias por su amable colaboración.

- Pendrives olvidados (Baiting): Es una técnica muy efectiva, que utiliza pendrives con malware para infectar la red de una Compañía:

  - Delincuente: Genera malware en varios pendrives.
    Los ubica en lugares de la Compañía para que los empleados se percaten fácilmente y procedan a recogerlos (ascensores, baños, pasillos, escritorios, etc.)

  - Víctima: Recoge el pendrive y lo primero que intenta realizar es conectarlo en su equipo de cómputo, para validar su contenido, en la mayoría de los casos por simple curiosidad.
    Al instalarlo en su equipo de trabajo, se ejecuta automáticamente el malware o al abrir el archivo de ofimática, multimedia o .pdf, que muchas veces están nombrados como: ascensos, nómina gerencial, confidencial, cargos a crearse, etc. Lo anterior, haciéndolos más atractivos para la víctima.

  - Delincuente: Al ejecutarse el malware, obtiene acceso, escala privilegios y lleva a cabo su fechoría (robo/destrucción de información).

  Otro escenario, sería el del delincuente solicitándole el favor a una recepcionista o asistente, que le permita imprimir la hoja de vida (CV) que tiene en su pendrive, porque tiene una entrevista y olvidó traerla. Resultado, equipo de cómputo infectado y por consecuente acceso del delincuente a la red.

- Llamada de la Alta Gerencia: Se presenta con la llamada a cargos básicos, pero con acceso a información relevante de la Compañía, donde el delincuente se hace pasar por una persona con un cargo importante, solicitando con mucha premura información:

  - Delincuente: Buenos días, le habla el “Gerente de Asuntos Legales” y me encuentro fuera de la oficina con el Gerente General “menciona el nombre real de la persona que ocupa este cargo”.

  - Víctima: Buenos días, cuénteme.

  - Delincuente: Requerimos con urgencia el reporte de los estados financieros de los clientes VIP de la Compañía, debido a que estamos en una Junta Directiva y la información la trajimos en un pendrive que no abre. La información la puede enviar al siguiente correo fulanito@gmail.com, quien

está gestionando las presentaciones. Le quedaremos eternamente agradecidos.

- Víctima: Envía la información solicitada, con la sensación de haber ayudado al gerente general de su trabajo.

- Colarse en las instalaciones de la Compañía (Tailgating / Piggybacking): Se presenta en repetidas oportunidades, debido al sentido de solidaridad y buena voluntad de los empleados. Sencillamente, el delincuente se infiltra aprovechando cuando el empleado abre la puerta de acceso o solicita le colabore con el acceso biométrico por que dejó su carnet o su huella está fallando:

  Primer escenario:

  - Víctima: Va entrando por la puerta (colocando su tarjeta de acceso o huella) para poder acceder.

  - Delincuente: Antes de cerrarse la puerta aprovecha e ingresa al mismo recinto.

  Segundo escenario:

  - Víctima: Va entrando por el molinete (colocando su tarjeta de acceso o huella) para poder acceder.

  - Delincuente: Aborda la víctima y le solicita muy amablemente, por favor le colabore que el sistema no le está leyendo su tarjeta de acceso o huella.

  - Víctima: Procede a ayudar al delincuente y le concede el acceso.

- Correos electrónicos con malware a cuentas corporativas: Donde los delincuentes buscan obtener acceso a información sensible o secuestrarla para solicitar dinero por su recuperación. Lo anterior, a través de malware:

  - Delincuente: Procede a elaborar correos que llaman la atención y causan gran interés a las víctimas, como los que se relacionan a continuación:

    - Correo de la DIAN (Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales) en Colombia, donde se observa que lo envían desde un correo personal y dirige a una URL distinta a la oficial:

De: DIAN [mailto:emssanarvillagarzon.885@gmail.com]
Enviado el: Tuesday, June 05, 2018 9:15 AM
Asunto: Fwd: INCUMPLIMIENTO EN DECLARACIÓN DE RENTA - DIAN

DIAN MINHACIENDA GOBIERNO DE COLOMBIA

Bogota 05 de junio del 2018

señor:
estimado contribuyente

Analizando nuestro sistemas de bases de datos hemos detectado irregularidades y anomalías en su declaración de renta correspondiente al año 2018.

Adjunto a esta notificación la factura correspondiente que usted deberá pagar, recuerde que el no pago oportuno de su factura incurriria en el proceso de cobro juridico

https://bit.ly/2jbndyk
Haga clic o pulse para seguir vínculo.

Ilustración 3: Ejemplo de correo con malware anexo - DIAN

- Correo de la FISCALIA, donde anexan un archivo comprimido para ser abierto con una contraseña trivial "1234" y así saltar controles de email Gateway y antivirus:

Fwd: COMUNICADO ESTABLECIDO

E/S EL PORTICO DISTRACOM <distracomelpc[redacted]om.co>
lun 27/03/2017 7:33 a.m.

Bandeja de entrada

8888888888888888888J... 55 KB

Por ningún motivo descargue el archivo adjunto, podría infectar su dispositivo con un software malicioso

1 archivos adjuntos (55 KB) descargar Guardar en OneDrive - ragged

FISCALÍA GENERAL DE LA NACIÓN

Radicado No 375477494745325
Oficio No 28-04-2017
Página 1 de 1
CITACION UNICA
BOGOTA D.C

La FISCALIA GENERAL DE LA NACIÓN y la doctora **ANDREA** [redacted], en su condición de fiscal 28 Seccional Delegada ante los Jueces Penales del Circuito de la ciudad Bogotá. Por medio del presente documento le informan:

Que la resolución de sucesión en su contra ha sido determinada y en consecuencia **solicitamos su presentación en este despacho judicial sin fallas el dia MIERCOLES 29 DE MARZO DEL 2017 A LAS 05:30 PM** con el fin de rendir indagatoria por los cargos de **FALSEDAD DE DOCUMENTOS PUBLICOS. SU ASISTENCIA ES OBLIGATORIA** (recuerde llevar su documento de identificación).

A continuación adjuntamos la información detallada acerca de su proceso y fechas de citación visualice el archivo adjunto:

Por motivos de seguridad el archivo se encuentra protegido con contraseña para visualizarlo deberá digitar la siguiente.
CLAVE: 1234

Ilustración 4: Ejemplo de correo con malware anexo - FISCALIA

- Correo de la Entidad Financiera, donde anexan un archivo comprimido para ser abierto con una

contraseña trivial “1234” y así saltar controles de email Gateway y antivirus:

Ilustración 5: Ejemplo de correo con malware – Entidad Financiera

- Correo de ICETEX (Instituto Colombiano de Crédito Educativo y Estudios Técnicos en el Exterior), donde anexan un archivo comprimido para ser abierto con una contraseña trivial “1234” y así saltar controles de email Gateway y antivirus:

Ilustración 6: Ejemplo de correo con malware - ICETEX

- Víctima: Proceder a descargar y abrir los archivos anexos, muchas veces sin tener una relación directa con la entidad relacionada en el correo.

- Acceso no autorizado a información sensible de una Compañía (Office Snooping): Se presenta muy a menudo por el descuido que tienen los empleados al tratar temas confidenciales, en pasillos, baños, ascensores y sitios públicos (cafeterías, restaurantes, clubes, entre otros), los cuales son escuchados por personal externo o delincuentes:

    - Víctima: Realiza comentarios sobre hitos estratégicos y/o confidenciales de los procesos y/o proyectos en los que se encuentra participando, en los lugares mencionados en el párrafo anterior.

    - Delincuente: Tan sólo escucha y está muy atento de obtener la mayor cantidad de información, que le servirá para venderla o utilizarla para generar nuevos vectores de ataque.

- Recolección de documentación y elementos electrónicos desechados (Dumspter Diving / Trashing): Que se presenta en las Compañías cuando están realizando la depuración de inventarios o simplemente uno de los empleados está realizando una limpieza esporádica y procede a desechar todo lo que según a su criterio ya no le sirve:

    - Víctima: Valida los activos de información (documentos impresos, CDs/DVDs, pendrives, entre otros) que ya no son relevantes para su gestión y procede a botarlos en la caneca de la basura.

    - Delincuente: Accede a los repositorios de basura de la Compañía y recolecta todos los documentos y dispositivos electrónicos que fueron desechados. Donde en la gran mayoría de los casos encontrará información confidencial, que le servirá para venderla o generar nuevos vectores de ataque.

En Personas:

- El embargo: Normalmente se presenta en hogares donde cuentan con el apoyo de un empleado doméstico (v.gr. señora del aseo, ama de llaves, mayordomo, jardinero, entre otros.):

    - Delincuente: ¡Le llamo de parte de su patrón(a) “Alex”, quien se dedica a “X oficio”, trabaja en “X empresa” y vive en la dirección “carrera x con calle y” a donde me estoy comunicando, él/ella está en graves problemas y necesita su colaboración urgente!

- Víctima: Claro, ¿dígame como le puedo colaborar a mi patrón(a)?

- Delincuente: Resulta que a su patrón(a) tiene líos judiciales lo van a embargar, por lo tanto, para que no lo afecten demasiado el señor “Pérez” con número de identificación “000”, llegará hoy a las “03:00 p.m.” con el camión de placas “000XXX” de color “verde”, para que puedan sacar la mayor cantidad de enseres y así, no le embarguen mayor cosa.

- Víctima: Entendido, estaré muy atento(a).

  Efectivamente, el señor “Pérez” con el número, camión y placas en mención se acerca a la hora acordada y la víctima gestiona el retiro de los enseres, pensando en que está ayudando a minimizar la afectación del embargo de su patrón(a). Por la noche llega el patrón(a) y el empleado doméstico con ínfulas de haber ayudado le informa que llevó la tarea según lo acordado.

- El sobrino/a capturado por la policía: Inicia con la llamada a un teléfono fijo o móvil y suele ejecutarse por dos delincuentes, el primero finge ser un(a) joven en llano y el segundo finge ser de las autoridades, comúnmente de la policía:

  - Delincuente (1): Inicia la llamada y tan pronto contestan, entra en llanto diciendo “tío(a)” en repetidas ocasiones.

  - Víctima: Al escuchar el llanto diciendo “tío(a)”, se preocupa y empieza a preguntar si habla con su “sobrino(a)” llamado “Pepito(a)”.

  - Delincuente (1): Sólo responde “sí con él/ella”, y con voz sollozante dice: “tío(a)” espérame en la línea te paso al “señor policía”.

  - Delincuente (2): Habla con el “Patrullero/Capitán/Coronel de la policía XXX”, resulta que estábamos llevando a cabo una requisa y encontramos en el maletín de su sobrino(a) un revolver, el cual, tiene un historial de criminalística y en este momento vamos a llevarlo(a) a la fiscalía.

  - Víctima: (Bastante confundida y sorprendida), solicita al policía que le brinde un mayor contesto de los hechos.

  - Delincuente (2): Indica que no hay nada que explicar, eso lo tendrá que hacer su sobrino(a) ante un juez. Pero, que sí lo desea y estaría de acuerdo, para evitarse el trámite legal, él (Delincuente) le puede colaborar y evitarle esta tragedia, sí le realiza una consignación de dinero a la mayor brevedad.

- La lotería/premio: Se presenta en su mayoría a través de correos electrónicos y redes sociales mediante la modalidad de scam o hoax:

    - Delincuente: Genera una historia en la cual se ofrece una lotería/premio para las personas que diligencien el formulario que se encuentra anexo en el mensaje. Donde solicita datos personales, información laboral y demográfica. En estos formularios suelen manejar los campos de correo electrónico y contraseña.

    - Víctima: Procede con el diligenciamiento del formulario esperanzado en ser el gran afortunado. Habitualmente, las personas suelen diligenciar su contraseña de acceso al correo electrónico, que en la mayoría de los casos es la misma contraseña que utiliza en sus redes sociales y hasta para sus transacciones financieras.

- El trasteo: Se presenta en su mayoría a través de SMS (mensajes de texto) y correos electrónicos mediante la modalidad de scam o hoax, donde identifican a posibles víctimas con familiares en proceso de mudarse:

    - Delincuente: Genera un mensaje donde afirma que se encuentra estancado pasando la frontera o saliendo de la ciudad con el "trasteo" de un familiar (de la víctima), relacionando el nombre, documento de identificación y el domicilio de éste familiar. Donde requiere una suma de dinero para poder hacerle llegar el "trasteo" de su familiar; de no acceder, procederá a deshacerse de las pertenencias en cualquier lugar.

- El ciclista/motociclista mecánico experto: Con frecuencia abordan a ciclistas/ motociclistas que se encuentran solos, buscando la conversación para ganar su confianza, hablando normalmente sobre eventos deportivos, fallas de mecánica frecuentes, repuestos, marcas, grupos de ciclistas/motociclistas, después de ganarse tu confianza ejecutan su fechoría:

    - Delincuente:
        - Escucho un ruido extraño en la cadenilla, tensor, motor (entre otros) de tu cicla/moto; a mí me pasaba hace un tiempo, pero no te preocupes conozco un truco para que se te arregle.
        - Se una maniobra que muy pocas personas en el mundo pueden hacer y te la puedo enseñar.
        -

    - Víctima: ¿Claro, dime cuál es?

- Delincuente: La verdad, lo sé hacer estando montado sobre la cicla/moto.

Tan pronto la víctima facilita su cicla/moto, el delincuente siempre lleva en sus manos un objeto que le entrega a la víctima y lo sostenga, para darle confianza que no se iría dejando sus pertenencias, sin embargo, tan pronto como le es posible el delincuente emprende la huida.

- Amigo en el exterior: Se lleva a cabo a través de correos electrónicos o redes sociales, dirigidos a amigos o familiares de personas que se encuentran viajando fuera de su país de origen, lo anterior, debido a que los delincuentes han identificado previamente, en su mayor parte ésta información, en redes sociales:

    - Delincuente: Suplantando al amigo o familiar de la víctima envía correo indicando: “nombre del familiar o amigo” por favor ayúdame, te comento que he extraviado o he sido víctima de un robo y he perdido mí pasaporte, dinero en efectivo y tarjetas de crédito, por lo que requiero de tu colaboración, para que a través de una operación de cambio me hagas llegar “XX dólares/euros” y así, poder acercarme a la embajada más próxima y poder regresar.

    - Víctima: Intenta comunicarse con su familiar o amigo afectado muchas veces sin éxito; otras veces sí, pero suele hacerlo a través del mismo correo o perfil de red social que el delincuente a hackeado. Finalmente, procede con la transferencia en pro de ayudar.

- Cancelación de compra con tarjeta de crédito: Se lleva a cabo a por llamadas a números de teléfono fijo o móvil, a través de la modalidad de visión:

    - Delincuente: Hola buenos días/tardes/noches “nombre de la víctima”. Mi nombre es “nombre ficticio”, le llamo del departamento compras del banco “nombre banco de la víctima” en referencia a una compra que en este momento están realizando con su tarjeta de crédito. Por lo anterior, necesito validar si usted es quien está realizando la compra.

    - Víctima: Suele responder de inmediato que él/ella no es quien está utilizando su tarjeta de crédito.

    - Delincuente: Para ganar más la confianza de la víctima, le confirma datos personales como el nombre completo, número de identificación y dirección de residencia. A lo que procede a solicitarle a la víctima que tenga a la mano su tarjeta de crédito para validar los siguientes datos:

        - Número en realce de la tarjeta de crédito.
        - Fecha de vencimiento.
        - Código de 3 cifras al respaldo de la tarjeta de crédito (cvv).

    - Víctima: Procede a entregar la información requerida, con el propósito de cancelar la compra que no está haciendo.

- Clonación tarjeta de crédito/debito: Se presenta en cajeros automáticos (ATMs), estaciones de gasolina, restaurantes, bares, entre otros establecimientos, donde los delincuentes adulteran los datafonos (Pin Pads) o instalan un dispositivo para clonar la información de las bandas magnéticas de las tarjetas de crédito/debito, a través de la modalidad de spinning:

    - Delincuente: Adultera o instala dispositivo lector de bandas magnéticas (skimmer) y adicional, una micro cámara para capturar el pin (contraseña) de la víctima.

    - Víctima: Ingresa su tarjeta debito/crédito y digita su pin (contraseña), llevando a cabo su transacción sin por menores.

    - Delincuente: Extrae la información de las tarjetas y procede a clonarlas, junto con los pines grabados, procede a efectuar el Cibercrimen/Ciberdelito.

- El estafador romántico: El delincuente simula estar interesado en una relación. Se dirige a las víctimas mediante plataformas de citas en línea, también utiliza las redes sociales con perfiles atractivos. Que señales le alertarán:

    - Alguien que ha conocido hace poco en internet, le manifiesta intensos sentimientos, y le solicita chatear por privado.

    - Su perfil en internet no coincide con lo que le cuenta y afirma.

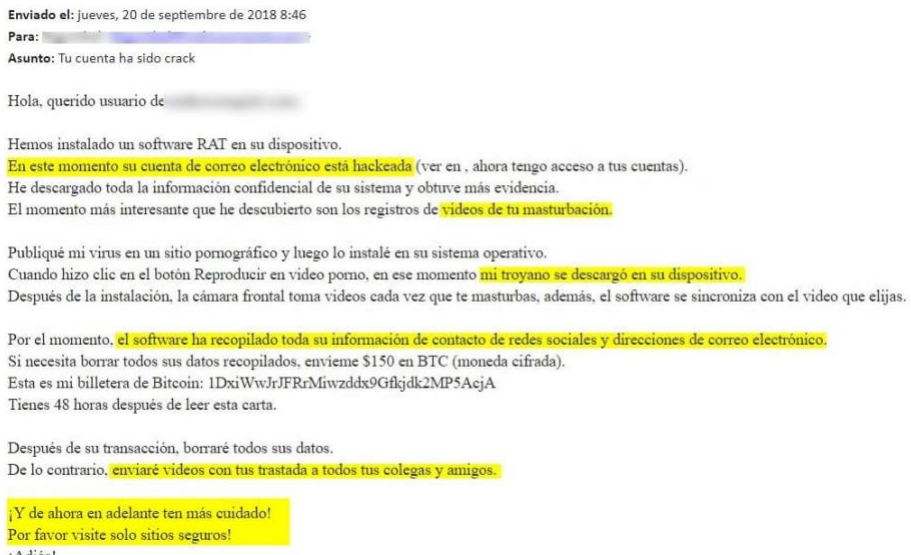
    - Le puede solicitar el envío de fotos o videos íntimos suyos.

    - Primero trata de ganar su confianza, después, le solicita dinero, regalos o los datos de sus cuentas bancarias o tarjetas de crédito. Sí no le envía dinero, procede a chantajearlo. Si le envía dinero le solicitará más.

    - Si usted es víctima, no se sienta avergonzado y cese inmediatamente todo contacto. Si es posible, guarde todas las conversaciones y presente una denuncia a la policía, informando la plataforma “online”, donde conoció al delincuente. Sí ha facilitado datos financieros, contacte a su banco de inmediato.

- Correo de Sextorsión: Donde el delincuente hace creer a la víctima que ha instalado un malware en su equipo de cómputo, interceptando su cámara web, micrófono y adicional ha robado las credenciales de su correo electrónico, para proceder a solicitarle un pago en criptomoneda para no divulgar la información recopilada:

    - Víctima: Recibe correo de Sextorsión con contenidos como se relaciona a continuación y lo más probable es que proceda a realizar el pago:



Enviado el: jueves, 20 de septiembre de 2018 8:46
Para: [redacted]
Asunto: Tu cuenta ha sido crack

Hola, querido usuario de [redacted]

Hemos instalado un software RAT en su dispositivo.
En este momento su cuenta de correo electrónico está hackeada (ver en , ahora tengo acceso a tus cuentas).
He descargado toda la información confidencial de su sistema y obtuve más evidencia.
El momento más interesante que he descubierto son los registros de videos de tu masturbación.

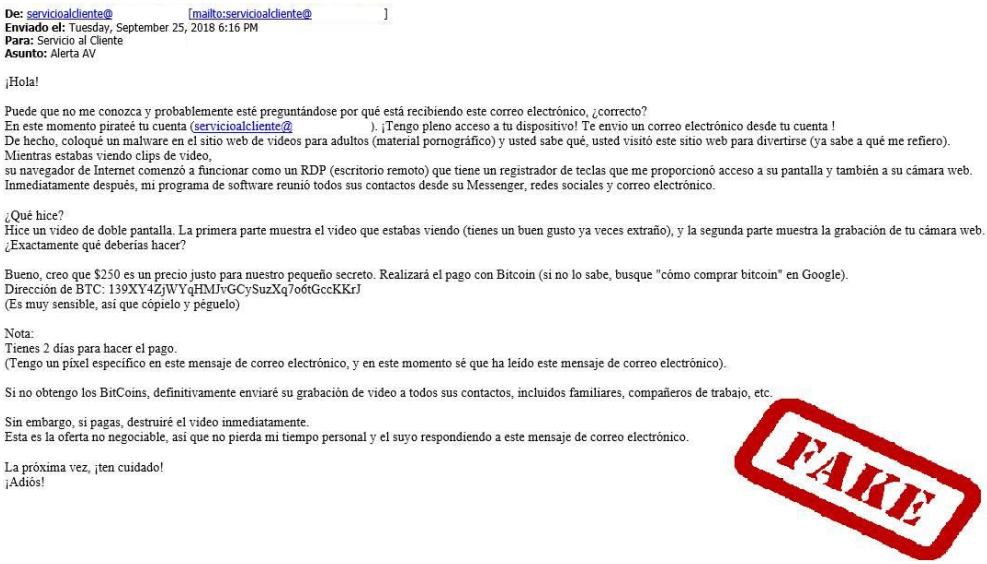
Publiqué mi virus en un sitio pornográfico y luego lo instalé en su sistema operativo.
Cuando hizo clic en el botón Reproducir en video porno, en ese momento mi troyano se descargó en su dispositivo.
Después de la instalación, la cámara frontal toma videos cada vez que te masturbas, además, el software se sincroniza con el video que elijas.

Por el momento, el software ha recopilado toda su información de contacto de redes sociales y direcciones de correo electrónico.
Si necesita borrar todos sus datos recopilados, envieme $150 en BTC (moneda cifrada).
Esta es mi billetera de Bitcoin: 1DxiWwJrJFRrMiwzddx9Gfkjdk2MP5AcjA
Tienes 48 horas después de leer esta carta.

Después de su transacción, borraré todos sus datos.
De lo contrario, enviaré videos con tus trastada a todos tus colegas y amigos.

¡Y de ahora en adelante ten más cuidado!
Por favor visite solo sitios seguros!
¡Adiós!

Ilustración 7: Ejemplo de correo Sextorsión



De: servicioalcliente@ [mailto:servicioalcliente@]
Enviado el: Tuesday, September 25, 2018 6:16 PM
Para: Servicio al Cliente
Asunto: Alerta AV

¡Hola!

Puede que no me conozca y probablemente esté preguntándose por qué está recibiendo este correo electrónico, ¿correcto?
En este momento pirateé tu cuenta (servicioalcliente@). ¡Tengo pleno acceso a tu dispositivo! Te envío un correo electrónico desde tu cuenta !
De hecho, coloqué un malware en el sitio web de videos para adultos (material pornográfico) y usted sabe qué, usted visitó este sitio web para divertirse (ya sabe a qué me refiero).
Mientras estabas viendo clips de video,
su navegador de Internet comenzó a funcionar como un RDP (escritorio remoto) que tiene un registrador de teclas que me proporcionó acceso a su pantalla y también a su cámara web.
Inmediatamente después, mi programa de software reunió todos sus contactos desde su Messenger, redes sociales y correo electrónico.

¿Qué hice?
Hice un video de doble pantalla. La primera parte muestra el video que estabas viendo (tienes un buen gusto ya veces extraño), y la segunda parte muestra la grabación de tu cámara web.
¿Exactamente qué deberías hacer?

Bueno, creo que $250 es un precio justo para nuestro pequeño secreto. Realizará el pago con Bitcoin (si no lo sabe, busque "cómo comprar bitcoin" en Google).
Dirección de BTC: 139XY4ZjWYqHMJvGCySuzXq7o6tGccKKrJ
(Es muy sensible, así que cópielo y péguelo)

Nota:
Tienes 2 días para hacer el pago.
(Tengo un píxel específico en este mensaje de correo electrónico, y en este momento sé que ha leído este mensaje de correo electrónico).

Si no obtengo los BitCoins, definitivamente enviaré su grabación de video a todos sus contactos, incluidos familiares, compañeros de trabajo, etc.

Sin embargo, si pagas, destruiré el video inmediatamente.
Esta es la oferta no negociable, así que no pierda mi tiempo personal y el suyo respondiendo a este mensaje de correo electrónico.

La próxima vez, ¡ten cuidado!
¡Adiós!

Ilustración 8: Ejemplo de correo Sextorsión_2

- Robo de credenciales a través de la clonación de páginas web (phishing), donde el delincuente lleva una copia casi exacta del sitio web con el cual la víctima se encuentra familiarizado. A continuación, se relacionan los siguientes ejemplos, que son

fácilmente identificables por la URL donde se encuentran hosteados:

- Facebook:

Ilustración 9: Ejemplo de phishing – FaceBook

- Netflix:

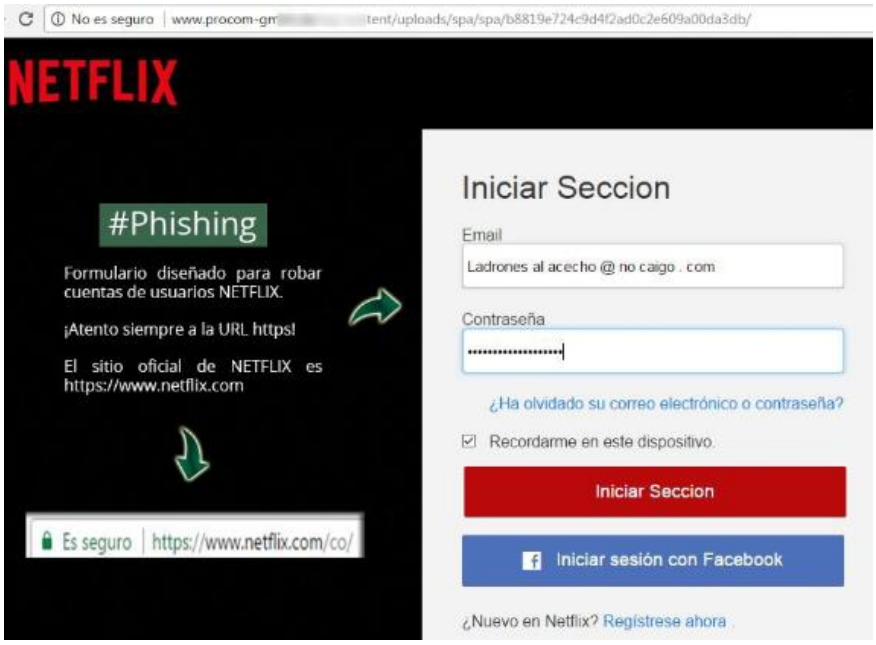


Ilustración 10: Ejemplo de phishing - Netflix

- Microsoft:

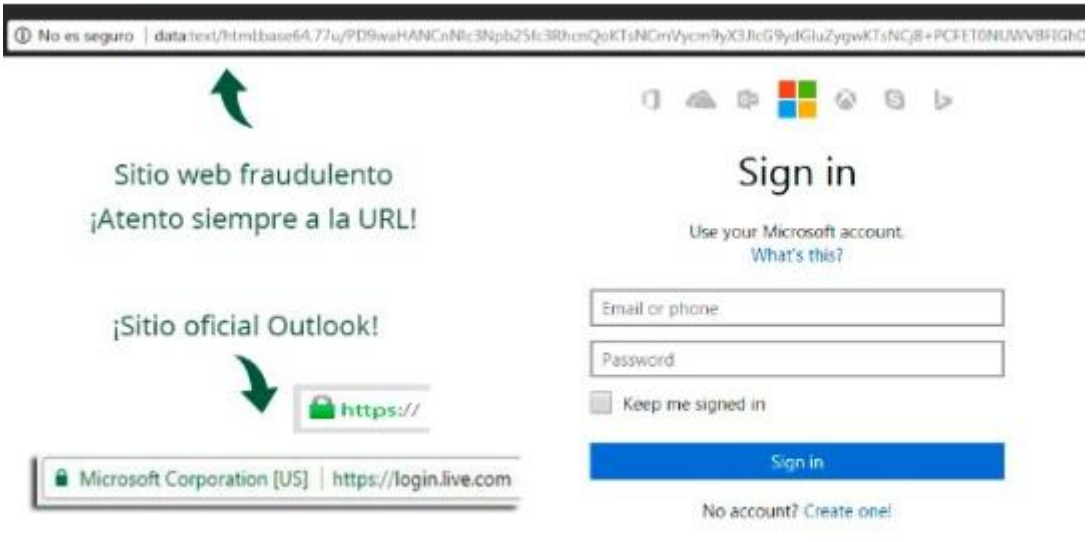


Ilustración 11: Ejemplo de phishing - Microsoft

- ¡El afortunado ganador! (smishing): A través de mensajes de texto (SMS), los delincuentes buscan llamar la atención de las víctimas a través de premios y rifas. Para que la víctima proceda a comunicarse y caer en las redes de la ingeniería social.

Ilustración 12: Ejemplo de Smishing – carroya.com

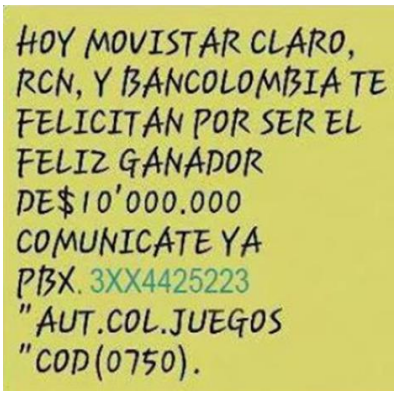


Ilustración 13: Ejemplo de Smishing – Coljuegos

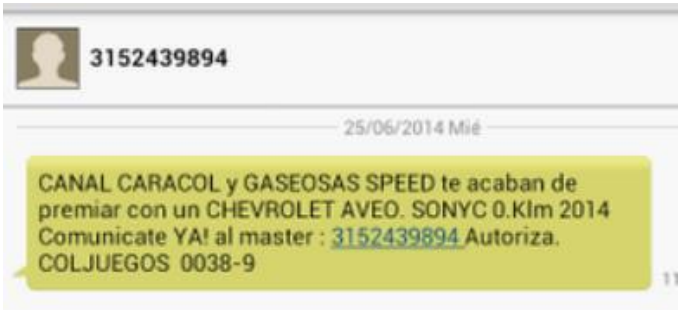


Ilustración 14: Ejemplo de Smishing - Coljuegos

- ¡Esta noticia es real! (Hoax): A través de mensajes en redes sociales y WhatsApp, los delincuentes buscan llamar la atención de las víctimas a través de atractivas ofertas, para que las víctimas accedan a los links y sean infectadas con malware de diferentes propósitos:

Ilustración 15: Ejemplo de Hoax - BurgerKing

Ilustración 16: Ejemplo de Hoax - Cinema

Ilustración 17: Ejemplo de Hoax - Netflix

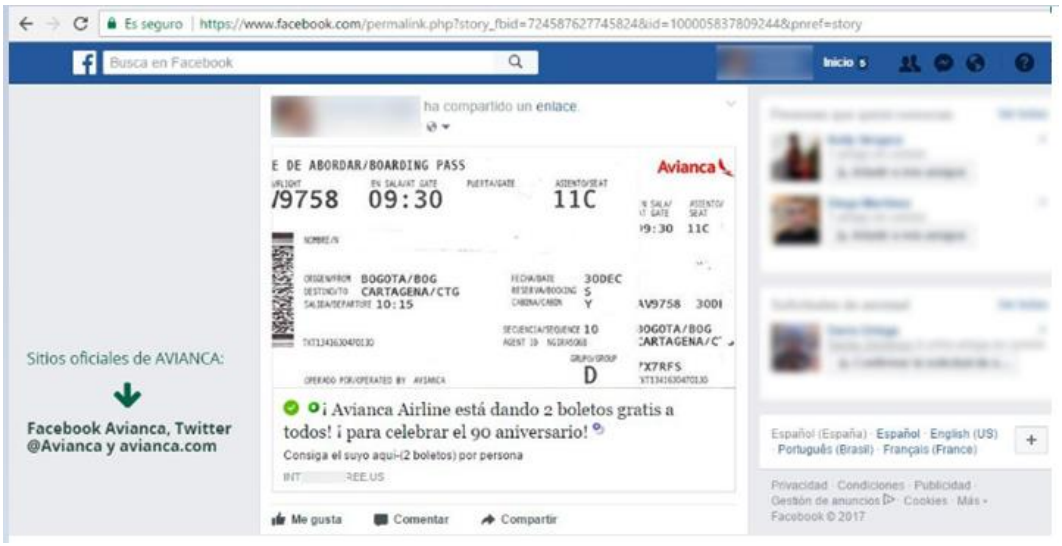


Ilustración 18: Ejemplo de Hoax – Avianca (FaceBook)

8. ¿Cómo poder evitar ser engañado mediante ingeniería social?

La principal recomendación para mitigar el riesgo de ser víctimas de la ingeniería social, tanto en el ámbito laboral como el personal es la concienciación y sensibilización continuas, sobre las técnicas de la ingeniería social, como funcionan y la afectación que puede llegar a presentar.

Es de vital importancia que las Compañías cuenten con un excelente centro de cómputo categorizado preferiblemente de nivel IV. Donde se lleve a cabo un esquema periódico de Backups (copias de respaldo) y cuenten con una excelente seguridad perimetral por capas:

Para Compañías:

- FW (Cortafuego perimetral) para que bloquee el acceso y salida de comunicaciones no autorizadas.

- WAF Web Application Firewall (Cortafuego de aplicación web) con el propósito de proteger los servidores de aplicaciones web de determinados ataques en la web.

- IDS/IPS (Sistema de detección/prevención de intrusos) para monitorear los paquetes de datos en las comunicaciones de la Compañía.

- Web Gateway (Puerta de enlace web) para filtrar la navegación que llevan a cabo los usuarios de la Compañía.

- Email Gateway (Puerta de enlace correo electrónico) para filtrar los correos electrónicos que gestionan los usuarios de la Compañía.

- Antivirus basado en heurística y no en firmas, es decir, por comportamiento, para identificar amenazas informáticas a priori y no dependiendo de los .dat que identifiquen las mismas.

- Actualizaciones y parches de seguridad para que los sistemas operativos, bases de datos, servicios web y equipos de comunicaciones mitiguen las brechas de seguridad en los mismos.

- Autenticación, para controlar el acceso a los sistemas de información con credenciales y contraseñas. En los casos de acceder a información sensible implementar el factor de autenticación doble.

- Perfilamiento de usuarios, basándose siempre en la necesidad de conocimiento y el mínimo privilegio.

- Cifrado de discos duros de equipos de cómputos, servidores y respaldos, para prevenir la fuga de información.

- Correlación de eventos, para llevar a cabo un correcto y acertado monitoreo de la red.

- VPNs, para llevar a cabo la comunicación externa de forma segura a los sistemas de información.

- Ten cuidado de tu entorno. Asegúrese de saber quién debe y no debe estar en sus instalaciones y de que hayan seguido los requisitos de ingreso

- Ve más despacio. La mayoría de los ataques transmiten un sentido de urgencia, así que haga una pausa y piense si lo que la persona está pidiendo es legítimo.

- En caso de duda sobre una orden de compra, pago, transferencia, consulta a tu Jefe/Gerente o superior.

- No abras enlaces o adjuntos sospechosos recibidos por correo. Ten mucho cuidado al consultar correos personales en el equipo de cómputo que te asigna la Compañía.

- No compartas información sobre el Organigrama, seguridad y procedimientos internos de la Compañía.

- Deja sólo absolutamente lo necesario en el escritorio, no dejes accesibles documentos impresos que contengan datos confidenciales, siempre guárdalos bajo llave.

- Asegura tu portátil (laptop) con guaya de seguridad, cada vez que te retires de tu puesto de trabajo.

- No dejes USBs, DVDs/CDs, u otro elemento de almacenamiento removible con información en lugares visibles y accesibles.

- No utilices sticky-notes, post-it y “papelitos” para anotar usuarios, contraseñas e información confidencial.

Para Personas:

- En sus equipos de cómputo y dispositivos móviles:

    - Antivirus, Firewall, Actualizaciones y parches de seguridad de su sistema operativo y Autenticación.

    - Ten mucho cuidado con la cantidad de información personal que compartes en sitios de redes sociales, recuerda siempre ser muy cauto. Los estafadores pueden utilizar tu información e imágenes para crear una identidad falsa o para apuntar con una estafa. Estos detalles pueden proporcionar a los piratas informáticos su ubicación, municiones para realizar ataques de phishing y respuestas a preguntas de seguridad. Piensa antes de compartir.

    - Tener una contraseña diferente y única para cada cuenta, lo suficientemente fuerte como para suponer que incluso su cónyuge no las puede deducir. A continuación, se relaciona tips para construcción de contraseñas, seguras, robustas y de fácil recordación:

        1. *A partir de una frase*: Piensa en una frase que tenga algún significado para ti y de ser posible para nadie más. Que no sea ni muy corta ni muy larga para que la puedas recordar fácilmente. Si tiene mayúsculas y números, mejor. Si hay algún símbolo magnífico. Ahora coge la primera letra de cada palabra. ¿No se te ocurre nada? Tranquilo, el título de tu canción, cuento o libro favorito puede ser un punto de partida. Ejemplos:

            - “El Coronel no tiene quien le escriba”, quedaría “**EcNtQlE++2**”. Me gustó tanto que lo leí dos veces de ahí que adicionara el símbolo “+” dos veces y el número 2.

- “El lobo feroz y los tres cerditos”, quedaría “**ElFyL3c--1**”. No me gustaba mucho ese cuento por eso adicioné el símbolo “-”.

2. *Combina dos palabras*: Elige dos palabras (de nuevo, mejor si significan algo sólo para ti) y construye otra alternando sus letras. Utilicemos como ejemplo el nombre “Laura Camila”, la base de tu nueva contraseña será “**LCaaumrilaa**”. No tiene números ni símbolos, así que tendrás que utilizarla como punto de partida para reforzarla con alguno de los otros métodos que voy a explicarte.

3. *Convierte las vocales en números*: Es un truco bastante popular que los ciberdelincuentes ya conocen y sortean, pero que puede funcionar muy bien para complementar alguno de los otros métodos. Retomando el ejemplo del punto anterior, nuestra clave provisional “**LCaaumrilaa**”, se convierte en otra un poco más segura: “**LC44umr1l44**”. Añadiendo uno o varios símbolos podría utilizarse.

4. *Sin vocales*: En lugar de reemplazarlas por números como en el ejemplo anterior, podríamos eliminar las vocales por completo. Si, utilizamos mi nombre como ejemplo “**AlejandroMéndezCarvajal**”, se convierte en una contraseña segura: “**AljndrMndzCrvjl**”. Cualquier parecido con una palabra real será difícilmente pura coincidencia, pero recuerda añadir números, mayúsculas y símbolos antes de emplearla.

5. *El truco del teclado*: Escoge un número fácil de recordar (por ejemplo, fecha de nacimiento de un ser querido). Supongamos que es **1950**. Ahora busca cada uno de los números en el teclado y vuelve a introducirlo seguido por las teclas que tiene justo debajo: “**1qaz9ol.5tgb0pñ-**”. Para complicarlo un poco más, cambia alguno de los caracteres por un símbolo e incluye alguna mayúscula.

6. *Una palabra y un número mezclados:* Elige palabras y números fácil de recordar, para hacerlo todavía más sencillo. Voy a usar “**Bigote**” y “**1950**”. El truco está en ir colocando las letras una a una, intercalando las cifras del número, pero a la inversa. Así: “**B0i5g9o1te**”, ya sabes lo que falta, ¿no? Usa un símbolo y listo.

7. *Camúflate con el entorno*: Usar la misma contraseña en varios aplicativos, es una terrible idea, no obstante, un truco sencillo puede hacer que tu clave se vuelva todo-terreno sin tener que recordar varios términos. Por ejemplo, si quieres registrarte en **Facebook**, ¿Qué puedes hacer? Incluye las siglas "**FB**" al inicio o al final de la clave (regular) que estás usando; añade una variación del nombre de la web con mayúsculas, símbolos y números (mucho mejor) o imagina y usa alguna referencia más sutil (excelente). Si lo aplicamos a nuestro ejemplo anterior, obtenemos las siguientes versiones:

    - **B0i5g9o1te_FB**
    - **F4c3b00k_B0i5g9o1te**
    - **Tw1t3rB0i5g9o1te**
    - **Inst4gr4mB0i5g9o1te**

- Mantenga sus cuentas comerciales separadas de sus cuentas personales.

- Cambia tus contraseñas a menudo, no las grabes todas en tus dispositivos móviles o equipo de cómputo. Puedes apoyarte en software licenciado y muy bien ranqueado para la administración de contraseñas, puedes consultar en internet.

- Gestiona una copia de seguridad de la información y configuración de tu computadora y dispositivos móviles.

- Revisar tus cuentas en línea con regularidad.

- Comprobar tu cuenta bancaria con regularidad y reportar cualquier actividad sospechosa a tu banco.

- Si una oferta parece demasiado buena para ser verdad, es casi siempre una estafa.

- Debes mantener tu información personal segura y protegida. No solicites ni provoques imágenes o videos íntimos, porque aunque tú no pretendas hacer mal uso de los mismos, pueden acabar en manos de otra persona, que sí termine por dañarte a ti, familiares o tus amistades.

- Si piensas que has proporcionado detalles de tus productos financieros a un estafador, ponte en contacto con tu entidad financiera inmediatamente.

- Recuerda siempre reportar, cualquier intento de fraude a las autoridades competentes, incluso si no eres víctima de la estafa

- Al usar su WiFi:

  - No permita que su dispositivo se una automáticamente a redes desconocidas.

  - Siempre apague el WiFi cuando no lo esté usando o no lo necesite.

  - Nunca envíe información confidencial a través de WiFi a menos que esté absolutamente seguro de que es una red segura.

- Al interactuar con Aplicaciones:

  - Solo use las aplicaciones disponibles en la tienda oficial de su dispositivo, nunca las descargue desde un navegador.

  - Desconfíe de las aplicaciones de desarrolladores desconocidos o de aquellos con revisiones limitadas/malas.

  - Si su tienda ya no los admite, simplemente elimínelos.

  - No le conceda administrador ni privilegios excesivos a las aplicaciones a menos que realmente confíe en ellas.

- Al utilizar un Navegador Web:

  - Cuidado con los anuncios, sorteos y concursos que parecen demasiado buenos para ser verdad. A menudo, estos conducen a sitios de phishing que parecen ser legítimos.

  - Preste mucha atención a las URL. Estos son más difíciles de verificar en las pantallas de dispositivos móviles, pero vale la pena.

  - Nunca guarde su información de inicio de sesión cuando esté utilizando un navegador web.

  - Preste atención a las advertencias que su navegador está parpadeando en su cara.

  - Realizar pagos en línea sólo en sitios web seguros (comprobar la barra de URL para el candado y HTTPS) y el uso de conexiones seguras (elije una red móvil en lugar de puntos de acceso Wi-Fi).

- Con el Bluetooth:
    - Desactivar el emparejamiento automático de Bluetooth.
    - Siempre apágalo cuando no lo necesites.
- Con los SMS:
    - No confíe en los mensajes que intentan que usted revele información personal.
    - Tenga cuidado con las tácticas similares en plataformas como WhatsApp, Facebook Messenger, Instagram, Twitter, etc.
    - Trate los mensajes de la misma manera que trataría el correo electrónico, siempre piense antes de hacer clic.
- Al recibir llamadas telefónicas:
    - No responda a las solicitudes de información personal o financiera por teléfono. Si está preocupado, llame directamente a la institución financiera, utilizando el número de teléfono que aparece en el reverso de su tarjeta de crédito o en su cuenta mensual.
    - Nunca suministre números de tarjetas de crédito, fechas de vencimiento, código de seguridad (CVV) y clave secreta (PIN).
    - A continuación te brindo tips para contestar el teléfono antes llamadas extrañas:

Preguntas de delincuentes	***Respuestas que debes dar***
¿Hola, a donde llamo?	¿A dónde está llamando?
¿Quién habla?	¿Con quién quiere hablar?
¿Eres tú primo?	¿Quién llama? Confírmeme su nombre y apellido
¿Soy tu primo “ABC”?	¿Hijo de cual de mis tío(a)s? (nombre y apellido)
Yo sé que usted tiene / es	Usted está mal informado
¡Usted se ha ganado un premio!	No he participado en ninguna rifa
Papá/mamá/tío(a), soy tu hijo(a)/sobrino(a) secuestrado (llama llorando)	¿Cómo se llama(n) tu(s) abuelo(a) (s)?
¡Lo tenemos vigilado!	¿Qué atuendo estoy usando?
Estamos recibiendo amenazas de este número	Realice el respectivo reporte ante las autoridades
Sal de tu casa/apartamento y dame los teléfonos de tus	Voy a llamar de inmediato a la policía

padres	
Lo llamo de… para actualizar sus datos	No, prefiero actualizar los datos personalmente en la oficina

- En correos electrónicos:

    - No haga clic en enlaces directos (en correos electrónicos, mensajes de texto, mensajes, etc.), especialmente en aquellos que le piden que ingrese información confidencial. Es mejor ir directamente a la fuente.

    - Esté muy atento a los errores ortográficos, gramaticales e historias incoherentes y pretextos.

    - Tu banco nunca le pedirá información confidencial como credenciales de su cuenta en línea a través del teléfono o correo electrónico.

9. Leyes a nivel mundial para perseguir las actuaciones de la ingeniería social.

Antes de identificar las leyes establecidas a nivel legal para perseguir las actuaciones de la ingeniería social ilícita se relaciona la siguiente definición del Departamento de Justicia de Estados Unidos: delito informático es cualquier acto ilegal cuya perpetración, investigación o acusación exige poseer conocimientos de tecnología informática. Se puede definir como todos los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos.

A continuación, se relacionan las leyes definidas en diferentes países para el tratamiento de delitos informáticos:

- Alemania: para hacer frente a la delincuencia relacionada con la informática y con efectos a partir del 1 de agosto de 1986, se adoptó la Segunda Ley contra la Criminalidad Económica del 15 de mayo de 1986 en la que se contemplan los siguientes delitos:

    - Espionaje de datos (202 a).

    - Estafa informática (263 a).

    - Falsificación de datos probatorios (269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos (270, 271, 273).

- Alteración de datos (303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.

- Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, Inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.

- Utilización abusiva de cheques o tarjetas de crédito (266b).

- Austria: Ley de reforma del Código Penal de 22 de diciembre de 1987. Esta ley contempla los siguientes delitos:

  - Destrucción de datos (126). En este artículo se regulan no solo los datos personales sino también los no personales y los programas.

  - Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además, contempla sanciones para quienes cometen este hecho utilizando su profesión.

- Francia: Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático.

  - Acceso fraudulento a un sistema de elaboración de datos (462-2). - En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.

  - Sabotaje informático (462-3). - En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.

  - Destrucción de datos (462-4). - En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.

- Falsificación de documentos informatizados (462-5). - En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.

- Uso de documentos informatizados falsos (462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

- Estados Unidos: adopción en los Estados Unidos en 1994 del Acta Federal de Abuso computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986.

- España: En España el tratamiento dado a este tema es abordado en el nuevo Código Penal de 1995 aprobado por Ley-Orgánica 10/1995, de 23 de noviembre y publicado en el BOE número 281, de 24 de noviembre de 1.995. A continuación, se hará una breve reseña sobre el contenido del Nuevo Código Penal Español en referencia a la penalización de la delincuencia informática:

  - Interceptación del Correo Electrónico. Art. 197.

  - Usurpación y cesión de datos Reservados de carácter personal. Art. 197.2 – Art. 18.3.

  - Fraude informático. Arts. 248 y siguientes.

  - Daños informáticos. Art. 264.2

  - Difusión de mensajes injuriosos o calumniosos. Arts. 211, 212.

  - Falsedades documentales. Arts.26, 390, 395 y 396.

  - Revelación de secretos. Art. 278.

  - Robos. Art. 239.

- Argentina: Ley 26.388, promulgada el 24 de junio de 2005. Ley 25.326 (2000). A partir de junio de 2008, la Ley 26.388 conocida como la “ley de delitos informáticos” ha incorporado y realizado una serie de modificaciones al Código Penal argentino.

  - Violación de datos personales. Art. 157 bis.

  - Difusión de Malware. Art. 183.

  - Difusión maliciosa de información. Art. 155.

  - Grooming. Art. 131.

- Brasil: Artículo 313ª, 313B del código penal brasileño. Ley 12.737 (2012), Ley 11.829 (2008). La Ley 12.737 es una ley reciente (año 2012), en la cual se dispone la tipificación criminal de los delitos informáticos y otras providencias.

    - Violación de datos personales. Art. 154-A Inc. 3.

    - Difusión de Malware. Art. 154-A Inc. 1.

    - Difusión maliciosa de información. Art. 154-A Inc. 4.

    - Grooming. Art. 131.

- Chile: En junio de 1993 entró en vigencia en Chile la Ley N°19.223, sobre delitos informáticos. La Ley Nº 19.223 tiene como finalidad proteger a un nuevo bien jurídico como es: “la calidad, pureza e idoneidad de la información en cuanto a tal, contenida en un sistema automatizado de tratamiento de la misma y de los productos que de su operación se obtengan”. Es una ley especial, extra código y consta de 4 artículos. Ley 20.009 (2005), Ley 18.168 (2002).

- Costa Rica:

    - Violación de datos personales. Art. 196 bis.

    - Difusión de Malware. Art. 232.

    - Difusión maliciosa de información. Art. 236. A.

    - Suplantación de identidad digital. Art. 230.

    - Grooming. Art. 167 A.

    - Captación o venta ilegitima de datos. Art. 196 bis y Art. 233.

    - Espionaje informático. Art. 231 y Art. 228.

- Ecuador: Ley 2002-67. La Ley No. 67/2002 regula el Comercio Electrónico, Firmas y Mensajes de datos. En dicha norma, dentro del Capítulo I del Título V, titulado "DE LAS INFRACCIONES INFORMÁTICAS", el art. 57 afirma que "Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley." En artículo siguiente, agrega y modifica varios artículos al Código Penal, incorporando diferentes figuras de delitos informáticos.

    - Violación de datos personales. Art. 202.2.

    - Hurto Informático. Art. 553.1.
    - Difusión maliciosa de información. Art. 202.1.
    - Violación a la intimidad. Art. 606.20.
- El Salvador:
    - Hurto Informático. Art. 208 Inc. 2.
    - Difusión maliciosa de información. Art. 184 y 185.
- Guatemala:
    - Violación de datos personales. Art. 274. D.
    - Difusión de Malware. Art. 274 G.
    - Violación a la intimidad. Art. 274 D.
- Honduras:
    - Hurto Informático. Art. 22.3
    - Difusión maliciosa de información. Art. 215.
- México:
    - Grooming. Art. 202.
- Nicaragua:
    - Violación a la intimidad. Art. 175.
- Panamá:
    - Grooming. Art. 187.
    - Agravantes. Art. 291 y 292.
- Perú: Ley 27.309 (2000), Ley 28.251 (2004). La Ley 27309 incorpora al Código Penal del Perú los Delitos Informáticos, a través de un artículo único que modifica el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo No 635, introduciendo allí los artículos 207 – A – B y C y 208. En otro orden, la Ley 28.251 actualizó e incorporó distintos delitos contra la integridad sexual, entre ellos, tipificando la pornografía infantil, a través de la modificación del art 183-A. Además, Perú posee la Ley 28.493 (2005) que regula el uso del correo

electrónico no solicitado (spam), sin embargo, en la misma no incluye ningún tipo de sanción penal.

    - Agravantes. Art. 207. C.

- Puerto Rico:

    - Violación de datos personales. Art. 167 y Art. 172.

    - Difusión de Malware. Ley de Espionaje Cibernético 1165/2008.

    - Hurto Informático. Art. 181.

    - Difusión maliciosa de información. Art. 173.

    - Suplantación de identidad digital. Art. 208 y 209.

    - Grooming. Art. 148.

    - Captación o venta ilegitima de datos. Art. 192.

    - Carding. Art. 205 y 229.

    - Espionaje informático. Ley de Espionaje Cibernético 1165/2008.

    - Violación a la intimidad. Art. 168 y 178.

- República Dominicana:

    - Difusión de Malware. Art. 8.

    - Difusión maliciosa de información. Art. 6 Párrafo I.

    - Suplantación de identidad digital. Art. 17.

    - Grooming. Art. 23.

    - Carding. Art. 5.

    - Espionaje informático. Ley de Espionaje Cibernético 1165/2008.

    - Violación a la intimidad. Art. 19.

- Bolivia: Código Penal, Ley 1.768 (1997), Ley 3325 (2006). La Ley 1.768 realiza una reforma general al Código Penal. Allí incorpora como Capítulo XI, del Título XII, del Libro Segundo del Código Penal, el de "DELITOS INFORMÁTICOS". entro de este capítulo,

se incorporan 2 artículos: 363 bis y ter, en cuyos textos se tipifica algunos delitos informáticos.

  - Artículo 363.Bis, 362 del código penal boliviano.

- Paraguay: Código Penal – Ley 1.160 (1997), Ley 2.861. se ha incorporado tipos penales específicos (como el caso del art. 175 de Sabotaje de Computadoras). Los artículos son 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249.

- Uruguay: Ley 18.600 (2009), Ley 17.520 (2002), Ley 17.815 (2004), Ley 18.383 (2008), Ley 18.515 (2009). El art. 7 de la Ley 17.815, afirma que “constituye delito de comunicación la comisión, a través de un medio de comunicación, de un hecho calificado como delito por el Código Penal o por leyes especiales.”, permitiendo así la aplicación de los tipos clásicos del CP. La Ley N° 17.520, penaliza el uso indebido de señales destinadas exclusivamente a ser recibidas en régimen de abonados. La Ley Nº 17.815 regula la violencia sexual, comercial o no comercial cometida contra niños, adolescentes e incapaces que contenga la imagen o cualquier otra forma de representación.

  - Difusión maliciosa de información. Art. 301 CP y Art. 8 de Ley 18.515.

- Venezuela: Ley 16002/1988 Articulo 129 y 130. Ley 16736/1996. Gaceta Oficial Nº 37.313 (2001). Posee una ley especial sobre Delitos Informáticos. Contiene 33 artículos y están clasificados en 5 Capítulos a saber: Contra sistemas que utilizan TI; Contra la propiedad; Contra la privacidad de las personas y las comunicaciones; Contra niños y adolescentes; Contra el orden económico.

  - Violación de datos personales. Art. 20.

  - Difusión de Malware. Art. 7.

  - Hurto Informático. Art. 13.

  - Difusión maliciosa de información. Art. 22.

  - Carding. Art. 16.

  - Espionaje informático. Art. 11.

  - Agravantes. Art. 27, 28 y 29.

- Colombia, solo hasta el 2009 se vino a tratar con rigurosidad el tema de la seguridad de la información con el nacimiento de la Ley 1273 de 2009, "Por medio de la cual se modifica el Código

Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". Ley 1366 (2009).

- Ley estatutaria 1266 del 31 de diciembre de 2008 “Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.

- Ley 1341 del 30 de julio de 2009 “Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”.

- Ley estatutaria 1581 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales”47. Su importancia radica en el tratamiento de la información personal, protegiéndola del uso indebido por parte de instituciones públicas o privadas. Su implementación y cumplimiento se ejecutan bajo el Decreto 1377 de 2013, en el que se establecen los mecanismos de protección necesarios para la protección de los datos de los usuarios.

A continuación, se relaciona cuadro de delitos informáticos en diferentes países:

País	Agravantes Especiales	Carding	Difusión de Malware	Difusión maliciosa de información	Espionaje informático	Estafa Informática	Gestión Ilegítima de datos	Grooming	Hurto Informático	Sabotaje Informático	Suplantación de Identidad Digital	Violación a la intimidad	Violación de Datos Personales
Alemania	-	Art.266.B	-	-	Art. 202.A	Art. 263.A	Art.269 - 270 - 271 - 273	-	-	Art.303.B	-	-	Art. 303.A
Argentina	-	-	Art. 183 2do párrafo	Art. 155	-	Art.148	-	Art. 131	-	-	-	-	Art. 157 bis
Austria	-	-	-	-	-	-	-	-	-	-	-	-	Art.126
Bolivia	Art. 362 Art. 363.Bis	-	-	-	-	-	-	-	-	-	-	-	-
Brasil	-	-	Art. 154-A Inc. 1.	Art. 154-A – Inc. 4	-	-	-	-	-	-	-	-	Art. 154-A Inc. 3
Chile	-	Art. 5 Ley 20.009.	-	Art. 4	-	-	-	Art. 366 quáter	-	-	-	Art. 161-A	-
Colombia	269 H	-	Art. 269 E	-	-	-	Art. 269G	-	Art. 269 I	-	-	-	Art. 269 F
Costa Rica	-	-	Art. 232	Art. 236. A	Art. 231 y Art. 288	-	Art. 196 bis. Y Art. 233	Art. 167. A	-	-	Art. 230	-	Art. 196 bis
Ecuador	-	-	-	Art. 202.1	-	-	-	-	Art. 553.1	-	-	Art. 606.20	Art. 202.2
El Salvador	-	-	-	Art. 184 y 185	-	-	-	-	Art. 208 inc. 2	-	-	-	-
España	-	-	-	Arts. 211, 212	Art. 197.	-	Art. 278	-	Art. 239	Art. 264.2	Arts. 248 Arts.26, 390, 395 y 396	-	Art. 197.2 Art. 18.3.
Estados Unidos	-	-	-	-	-	-	-	-	-	18 U.S.C. Sec.1030	-	-	-
Francia	-	-	-	-	-	Ley número 88-19 de 5 de enero de 1988	Art.462-2-5	-	-	Art.462-3	Art.462-6	-	Art.462-4
Guatemala	-	-	Art. 274 G	-	-	-	-	-	-	-	-	Art. 274 D	Art. 274 D
Honduras	-	-	-	Art. 215	-	-	-	-	Art. 223	-	-	-	-
México	-	-	-	-	-	-	-	Art. 202	-	-	-	-	-
Nicaragua	-	-	-	-	-	-	-	-	-	-	-	Art. 175	-
Panamá	Art. 291 y 292	-	-	-	-	-	-	Art. 187	-	-	-	-	-
Paraguay	Art. 144, 146, 173 a 175, 188, 189, 220, 239, 248 y 249.	-	-	-	-	-	-	-	-	Art. 175	-	-	-
Perú	Art. 207 C	-	-	-	-	-	-	Art. 183-A	-	-	-	-	-
Puerto Rico	-	Art. 205 y Art. 229	Ley de Espionaje Cibernético 1165/2008	Art. 173	Ley de Espionaje Cibernético 1165/2008	-	Art. 192	Art. 148	Art. 181	-	Art. 208 y Art. 209	Art. 168 y Art. 178	Art. 167 y Art. 172
Republica Dominicana	-	Art. 5	Art. 8	Art. 6 Párrafo I	-	-	-	Art. 23	-	-	Art. 17	Art. 19	-
Uruguay	-	-	-	Art. 301 CP y Art. 8	-	-	-	Art. 7	-	-	-	-	-
Venezuela	Art. 27, 28 y 29	Art. 16	Art. 7	Art. 22	Art. 11	-	-	-	Art. 13	-	-	-	Art. 20

Ilustración 19: Cuadro de delitos informáticos

10. Conclusiones

- Actualmente, no existe tecnología en el mundo que proteja a las personas, contra los diferentes ataques de ingeniería social. Siempre estaremos expuestos, por eso depende de nosotros mismos, identificar el vector de ataque y siempre estar muy alertas para utilizar como nuestra mejor defensa el sentido común.

- En muchos países del mundo, aún existen delitos informáticos que no se encuentran correctamente especificados en las leyes y código penal. Esta falencia deja sin argumentos a los entes regulatorios para judicializar a los ciberdelincuentes.

- La Ingeniería Social se ha convertido en el vector de ataque más exitoso para obtener información y lo seguirá siendo por la poca existencia de campañas de sensibilización y concienciación que hoy en día se ejecuta tanto en Compañías, como organizaciones gubernamentales. Por lo anterior, es de vital importancia que las personas tengan principios en ciberseguridad y estén preparadas para afrontar la ingeniería social.

- Este trabajo final de master será de gran aporte y de apoyo para que las personas adquieran las bases que les permitirá ser más conscientes y mitigar el riesgo de ser víctimas de la ingeniería social.

11. Glosario

- Activo de información: Toda aquella información que reside en medio electrónico o físico que tiene un significado y valor para la Compañía y, por ende, necesita ser protegida. Los activos de información incluyen la información estructurada y no estructurada que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico, almacenada electrónicamente en equipos de cómputo, memorias, dispositivos móviles, microfilmación, cintas o cualquier medio magnético u óptico, entre otros.

- Amenazas: Son eventos que pueden presentar incidentes en las Compañías, ocasionando una afectación de tipo material o en los activos de información. Las amenazas pueden ser:

    - Actor humano usando medios técnicos de forma deliberada o accidental, tanto externo como interno.

    - Actor humano usando medios físicos de forma deliberada o accidental, tanto externo como interno.

    - Problemas técnicos:
        - Defectos de software.
        - Defectos de hardware.
        - Caídas del sistema.
        - Código malicioso.

    - Otros problemas:
        - Suministro de energía.
        - Telecomunicaciones.
        - Terceras partes.
        - Desastres.

- Aplicación engañosa: Las aplicaciones engañosas pueden introducirse sigilosamente en su equipo cuando navega por la Web. Una vez instaladas, los estafadores las utilizan para cometer fraudes y robos de identidad.

- Autenticación**:** Proceso en el cual un usuario se registra a un sistema informático.

- Ciberseguridad: Condición caracterizada por un mínimo de riesgos y amenazas a las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones en el ciberespacio.

- Cibercrimen: Actos delincuenciales en el ciberespacio donde el principal objetivo es cometer ilícitos contra individuos, organizaciones y empresas.

- Ciberdelito: Operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

- Cifrado o encriptado de información: Método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

- Confidencialidad: Característica de la información que permite que sea accesible sólo a aquellas personas autorizadas.

- Contraseña**:** Es una serie de caracteres conocida sólo para un usuario que le permiten tener acceso a un sistema informático.

- Cookie: Archivos que se guardan en los equipos para que los sitios web recuerden determinados datos.

- Cuenta de usuario: Corresponde a los campos necesarios para realizar la identificación de un usuario en algún sistema informático.

- Dato Personal: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Existen diferentes tipos de datos personales:

    - Datos Públicos: Es el dato calificado como tal según los mandatos de la ley o de la constitución política y aquel que no sea semiprivado, privado o sensible. Son públicos, entre otros, cédula, nombre, los datos relativos al estado civil de las personas a su profesión u oficio, a su calidad de comerciante o servidor público y aquellos que puedan abstenerse sin reserva alguna. Por su naturaleza los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

    - Datos Privados: Son los datos que por su naturaleza intima o reservada solo son relevantes para el titular, por ejemplo, su fotografía o su correo electrónico personal son datos privados, estos pueden ser sensibles o no sensibles.

    - Datos Semiprivado: Es un dato semiprivado el dato que no contiene naturaleza íntima, reservada, ni publica y cuyo conocimiento y divulgación pueden interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

- Datos Sensibles: Se entiende por dato sensible aquellos que afecten la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, vida sexual y los datos biométricos (aquellos aspectos físicos que, mediante un análisis técnico, permiten identificar las características físicas y singulares de una persona, resultando que es imposible la coincidencia de tales aspectos en dos individuos. Así emplean para tal fin las huellas digitales, el iris del ojo, la vos entre otros). Los datos sensibles están dentro del grupo de datos privados.

- Delito Informático**:** Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

- Disponibilidad**:** Característica que permite que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, cada vez que lo requieran.

- HTTP (HyperText Transfer Protocol: Es un sistema de comunicación que permite la visualización de páginas Web, desde un navegador.

- Impacto: Es el nivel de afectación que se presenta cuando una amenaza explota una vulnerabilidad y se ésta se materializa. Existen 2 tipos:

  - Cuantitativos: Hace referencia a pérdidas económicas.
  - Cualitativos: Hace referencia a pérdidas funcionales u orgánicas.

- Exploit: Un error en el software que representa una brecha de seguridad.

- Extorsión: El uso de Internet para amenazar con la intención de extorsionar a un individuo para conseguir dinero u otra cosa de valor.

- Extensión: Los ficheros se representan asignándoles un nombre y una extensión, separados entre sí por un punto: *NOMBRE.EXTENSIÓN*.

- Incidente Informático: Es la violación o amenaza que afectan la confidencialidad, disponibilidad y la integración como la continuidad de los servicios que son ofrecidos.

- Información**:** Es la interpretación que se da a los datos, los cuales tienen un significado o valor. La información puede estar en medio físico o electrónico.

- IP (Internet Protocol) / TCP-IP: La IP es la dirección o código que identifica exclusivamente a cada uno de los ordenadores existentes.

- Keylogger: Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

- Malware**:** Término que proviene de las palabras **mal**icious – soft**ware** y engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos, Gusanos, keyloggers, Botnets, Ransomware, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues.

- Mitigar el riesgo: Previamente identificado y validado el riesgo, se basa en la gestión de llevar a cabo la implementación de controles que disminuyan la probabilidad o impacto del riesgo.

- Pruebas de Intrusión o Vulnerabilidades**:** pruebas que se ejecutan sobre recursos de TI, a fin de identificar posibles debilidades y establecer planes de acción para mitigar los riesgos asociados.

- Riesgo: Es la posibilidad de que una amenaza se produzca explotando una vulnerabilidad, dando lugar a un ataque y por consecuente un impacto.

- Rootkits**:** Es un juego de herramientas (programas) que permiten acceder a los niveles administrativos de un ordenador o una red.

- Seguridad de la Información: Es la preservación y protección de la confidencialidad, integridad y disponibilidad de la información, de una amplia gama de amenazas, con el objetivo de minimizar el daño, garantizar la continuidad operacional y maximizar el retorno sobre las inversiones y las oportunidades de los negocios de la compañía.

- Toolkit**:** Son programas de software que pueden usarse tanto por novatos como por expertos para facilitar el lanzamiento y distribución de ataques a computadoras en red.

- Usuario**:** La persona que tiene asignada credenciales con acceso a aplicaciones y sistemas de información de la Compañía.

- Vulnerabilidades: Hace referencia a la probabilidad que una amenaza se materialice sobre un activo de información, explotando la misma. Existen dos tipos:

- Vulnerabilidad Intrínseca: Es la que no contempla controles sobre el activo de información.

- Vulnerabilidad Efectiva: Es la que contempla controles sobre el activo de información.

12. Bibliografía

- https://es.scribd.com/document/74330995/La-Ingenieria-Social
- https://es.ccm.net/contents/25-ingenieria-social
- https://www.ecured.cu/Hacker
- https://www.24horas.cl/tendencias
- http://www.reydes.com/d/?q=Realizar_un_Ataque_de_Ingenieria_Social
- http://fortune.com/2017/10/25/cybercrime-spyware-marketplace/
- http://www.conasa.es/blog/seguridad/ingenieria-social-el-arte-de-obtener-informacion-confidencial/
- https://www.segurosenlared.co/8-general/2-ingenieria-social-el-arte-del-engano-en-la-red
- http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/
- https://www.onemagazine.es/one-hacker-consejos-para-que-quieren-datos-ciberdelincuentes
- https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf
- http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/
- https://www.eltiempo.com/archivo/documento/CMS-16020156