Proyecto de Grado

Instituto Universitario Aeronáutico
Facultad Ciencias de la Administración
Ingeniería en Sistemas

Tema: *Ingeniería Social, el arte de engañar.*

Profesor Tutor: Lic. Mira, Natalia Carolina

Equipo de Proyecto	Email
Paesani Lagger, María Belén	mpaesani353@alumnos.iua.edu.ar
Stucher, Vanesa Paola	vstucher940@alumnos.iua.edu.ar

Facultad de Ciencias de la Administración

Departamento Desarrollo Profesional

Lugar y fecha:.....

INFORME DE ACEPTACIÓN del PROYECTO DE GRADO

Título del Proyecto de Grado:.....

.....

Integrantes: (Apellido, Nombre y Carrera).....

.....

Profesor Tutor del PG:.....

Miembros del Tribunal Evaluador:.....

.....

Resolución del Tribunal Evaluador

☐ El PG puede aceptarse en su forma actual sin modificaciones.

☐ El PG puede aceptarse pero el/los alumno/s debería/n considerar las Observaciones sugeridas a continuación.

☐ Rechazar debido a las Observaciones formuladas a continuación.

Observaciones:

.....
.....
.....
.....
.....
.....
.....
.....
.....

Declaración de derechos de autor

Agradecimientos

Agradecemos a nuestras familias que nos apoyaron, que fueron nuestro soporte y nos brindaron su colaboración, alentándonos en cada paso.

A las autoridades, profesores y alumnos del colegio San José, de San Agustín por brindarnos su ayuda para llevar a cabo este proyecto.

También queremos agradecer a los profesores, que con mucha dedicación nos acompañaron estos años, guiándonos y preparándonos para esta profesión, la que elegimos y disfrutamos.

Dedicatoria

Este proyecto esta dedicado a Alejandro, Paula y mi familia. Ma. Belén

Este proyecto esta dedicado a Claudio y mi familia. Vanesa

Resumen o Abstracto

La Ingeniería Social se sustenta en el principio de que en cualquier sistema *"los usuarios son el eslabón más débil"*. Esto se traduce a que resulta más sencillo atacar a una persona y obtener información o una acción de ésta, que lograr vulnerar un sistema de información que se encuentra asegurado, blindado y protegido ante posibles ataques.

Se describieron los casos en los que se ha aplicado Ingeniería Social, con las explicaciones de cada uno y las recomendaciones a los usuarios para que no sean la próxima víctima de un Ingeniero Social.

Nuestro trabajo se orientó a alumnos de nivel medio, cuyas edades están comprendidas entre 12 y 18 años, de una Institución educativa de la provincia de Córdoba.

Al hacer Ingeniería Social, los nombres de figuras o empresas conocidas y las noticias de importancia utilizadas para fraguar el engaño se actualizan constantemente, así como se renuevan los temas a los que se recurre para generar confianza en el usuario. *El desconocimiento y la curiosidad son las vulnerabilidades que la Ingeniería Social explota*.

Por eso es importante que los usuarios se informen y eduquen. No todo aquello que es recibido por Internet, desde cualquier medio, es fidedigno y, si no fue solicitado, hay grandes posibilidades de que se trate de un intento de engaño.

Se diseñó un sitio Web, con actividades que fueron elaboradas con la asesoría psicopedagógica, como una herramienta para informar a los adolescentes. Además, se pretende en un futuro llevar a cabo la ejecución de talleres informativos. Se busca dejar planteado un camino a seguir para futuras investigaciones que puedan contribuir a mejorar la problemática abordada en este proyecto.

Índice

Índice de Figuras

1. Introducción

1.1. Antecedentes

"Si crees que la tecnología puede resolver tus problemas de seguridad, entonces no entiendes los problemas y no entiendes la tecnología".
Bruce Schneier.

En el campo de la Seguridad Informática, la Ingeniería Social se conoce como la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Podemos definir Ingeniería Social como el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros.

El desarrollo de ataques de Ingeniería Social resulta más efectivo acudiendo a las ventajas de la anonimidad, virtualidad y desconocimiento del usuario. *Conocer cómo trabaja es saber defenderse de ella.*

La Ingeniería Social se sustenta en el principio de que en cualquier sistema *"los usuarios son el eslabón más débil"*. Esto se traduce a que resulta más sencillo atacar a una persona y obtener información o una acción de ésta, que lograr vulnerar un sistema de información que se encuentra asegurado, blindado y protegido ante posibles ataques.

La Ingeniería Social está viviendo un verdadero auge, alentada por algunos factores en crecimiento como lo tecnológico, la movilidad y conectividad y redes sociales. Sin duda este crecimiento, favorece a las técnicas orientadas al engaño.

Es necesario deshacerse de la visión tan habitual "eso a mi no me va a pasar". Las nuevas tecnologías de por sí, son muy importantes y de gran relevancia en la educación de nuestros adolescentes, pero como en otras muchas

cosas en la vida real, hay que saber usarlas de forma correcta y enseñarles a que así lo hagan.

Lamentablemente muchos estudios muestran que los usuarios tienen una pobre conciencia acerca de la importancia de la seguridad. Las entrevistas desarrolladas por las personas que integran el presente proyecto, aportaron como resultado que el 85 % de los adolescentes comprendidos entre los 12 y 18 años, desconocen o tienen escasos conocimientos sobre Ingeniería Social y sus consecuencias (se desarrollará con mayor detalle el resultado de las encuestas realizadas a los alumnos y a los docentes de la Institución a lo largo del proyecto).

Otra encuesta de InfoSecurity arrojó como resultados que 90% de los oficinistas revelarían una clave de acceso a cambio de un bolígrafo.

El objetivo de este proyecto, es concientizar al usuario respecto a la Ingeniería Social. Para alcanzar dicho objetivo, debemos preparar al usuario, suministrándole información y conocimientos, para que pueda reconocer y evitar ataques de Ingeniería Social.

Nuestro trabajo estará orientado a alumnos de nivel medio, cuyas edades están comprendidas entre 12 y 18 años, de una Institución educativa de la provincia de Córdoba.

1.2. Situación Problemática

¿A cuántas personas conocemos que nos han dicho que le atacaron su cuenta de correo? ¿O que alguien se hizo pasar por otra persona en el Facebook para engañarle? ¿O que sencillamente alguien se metió en su Banco Virtual y le limpió la cuenta?. Pues esas personas han sido víctimas de la llamada “Ingeniería Social”.

Cuando hablamos de Seguridad de la Información muchas veces nos olvidamos del usuario final, quien por lo general es el blanco de los delincuentes.

La gran cantidad de riesgos existentes en Internet, en las redes sociales y a esto sumado que la Ingeniería Social se ha convertido en uno de los métodos

de ataque más frecuentes en nuestros días, es evidente lo expuesto que queda el usuario a estos peligros.

Se puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Parece que está todo bajo control. Pero no es así, ya que los seres humanos, seres a los que *no se los puede configurar*, deben ser capaces y responsables de filtrar y eliminar las peticiones malintencionadas.

¿Los usuarios están preparados?

Lo mejor es educar los sobre las técnicas de Ingeniería Social empleadas comúnmente para atacarlos.

1.3. Problema

La capacidad del usuario de conocer y poder evitar ser víctima de engaños es menor a la velocidad con la que las técnicas de Ingeniería Social evolucionan. Esto genera la necesidad de introducir cambios que apunten a que los usuarios tomen conciencia y estén mejor preparados para reconocer y evitar rápidamente ataques de Ingeniería Social.

1.4. Objeto de Estudio

El objeto de estudio es la Ingeniería Social y cómo ésta afecta al eslabón más débil de la cadena, es decir, al usuario.

1.5. Campo de Acción

El campo de acción se centrará en el estudio de Ingeniería Social y las técnicas de engaños más utilizadas favorecidas por el crecimiento tecnológico, movilidad, conectividad y redes sociales. Se desarrollará una página Web, que se utilizará en los espacios curriculares de la Institución Educativa. Dicha página Web será utilizada por docentes y alumnos del nivel medio del Colegio San José en la localidad de San Agustín.

1.6. Objetivos

1.6.1. Objetivo general

El objetivo que se persigue con este proyecto de investigación, es estudiar e identificar los riesgos a los que pueden verse sometidos los alumnos, conocido como Ingeniería Social, otorgando un conjunto de herramientas que permitan analizar, interpretar y evaluar los peligros que puedan afectar a los jóvenes. Para que éstos desarrollen capacidades críticas y reflexivas respecto al uso de Internet y las nuevas tecnologías de información y comunicación, y a su vez orientar a padres y docentes para que acompañen este desafío.

Para alcanzar este objetivo, se desarrollará una página Web, en la que se encontrarán guías, videos tutoriales, consejos, videos con información y actividades para los alumnos. Las actividades se elaborarán en cooperación con una asesora pedagógica de la Institución.

A futuro, se llevarán a cabo talleres de capacitación en la comunidad educativa (alumnos, docentes y padres), haciendo uso de la página Web elaborada por las tesistas, las actividades de dicha página, y otros materiales didácticos para crear un espacio de comunicación y participación con alumnos, docentes y padres de la Institución.

1.6.2. Objetivos específicos

Desarrollar una investigación y contextualización de:

- Realización de encuestas y procesamiento de los datos.
- Conceptos relevantes de la seguridad informática.
- Conceptos de la Ingeniería Social.
- Importancia del estudio de la Ingeniería Social.
- Técnicas de Ingeniería Social.
- Conceptos de Redes Sociales.
- Relación de las Redes Sociales y la Ingeniería Social.
- Analizar ejemplos de ataques de Ingeniería Social actuales.
- Construir una página Web.
- Realizar actividades para los alumnos en cooperación con asesoría pedagógica.
- Generar conclusiones pertinentes.

1.7. Idea a Defender / Propuesta a Justificar / Solución a Comprobar

A través de este proyecto de grado, se buscará definir y desarrollar los principios y fundamentos de la Ingeniería Social y sus implicancias con el uso de las nuevas tecnologías de información y comunicación.

Cualquier atacante puede engañar con facilidad a un usuario ingenuo. Por eso es importante que estemos debidamente educados, capacitados e informados para estar alertas, anticiparnos al engaño y evitar así ser víctimas de un ataque de Ingeniería Social.

Se propone por tanto el desarrollo de una página Web, orientada al nivel medio y docentes de una Institución educativa, apuntando a la protección de datos personales, de intimidad y de privacidad en Internet en relación a la prevención y detección de riesgos y amenazas de la Ingeniería Social.

1.8. Delimitación del Proyecto

En este proyecto se va a realizar un análisis teórico, con una ejemplificación actual y pertinente en cada caso sobre la Ingeniería Social, que se

plasmará en la página Web. Orientado a adolescentes de 12 a 18 años, contando con la participación de los docentes del Colegio San José.

1.9. Aporte Práctico

Se espera que los resultados de este proyecto tengan un impacto dentro y fuera de la comunidad del Colegio San José. Y que sirvan a todos los usuarios que día a día utilizan Internet, ya que pueden ser las siguientes víctimas.

Hemos encontrado noticias en donde se ve de manifiesto el engaño utilizando Ingeniería Social. Algunos fragmentos son los siguientes:

- Engañada por Facebook, casi sufre calvario; Una adolescente cordobesa de 14 años fue manipulada por un hombre que simuló ser una niña rosarina. Al ganar su confianza, logró que la menor le enviara fotos íntimas. Publicado por el diario La Voz del Interior, 28 Agosto 2013.
- "El fraude a través de Internet", información recopilada durante el primer cuatrimestre de 2012 sobre una base de 3.646 internautas y 7.723 análisis remotos. Los resultados se han obtenido con un nivel de confianza del 95,5%. Elaborado por INTECO, 28 Enero 2013.
- Las formas más habituales de intento de fraude directo al usuario son:

Formas adoptadas por el remitente según el tipo de comunicación sospechosa que ha experimentado el internauta (%)

Tipo de incidencia declarada	Forma adoptada por el remitente de la comunicación										
	Banco	Comercio electrónico	Loterías	Particular	Redes sociales	Medios de pago	Subastas	Telecomunicaciones	ONG y fundaciones	Administraciones	Otros
Recepción de e-mail solicitando claves de usuario	**69,6**	21,2	13,9	9,0	14,3	21,0	7,9	10,3	6,5	7,0	5,0
Recepción de e-mail ofertando un servicio no solicitado	25,9	**41,3**	28,2	14,5	19,7	14,0	14,2	16,3	8,1	5,7	8,0
Recepción de e-mail con invitación a visitar alguna página web sospechosa	25,6	**30,0**	28,2	23,4	19,9	13,1	15,6	12,0	8,3	5,6	10,5
Recepción de una oferta de trabajo por Internet que pudiera ser falsa o sospechosa	9,0	13,7	8,6	**36,1**	16,5	7,7	6,4	8,4	10,0	10,0	20,6

Ilustración 1- Formas habituales de intento de fraude al usuario

- Policía encubierto en Facebook da una lección a adolescentes. La inseguridad en Facebook es cosa de todos los días. Son bien conocidas las diferentes formas de engaño que circulan en la red social, pero uno de los mayores peligros es la ingeniería social, ese método que usan lo criminales para sacarle información a las personas sin usar programas o cualquier tipo de software. Para concientizar a la gente, en especial a los jóvenes, un policía canadiense se hizo pasar por adolescente en la red social y se dedicó a obtener información sensible de sus contactos. Darren Laur, un policía canadiense de 46 años, se dedicó a investigar sobre cómo se movían los jóvenes en su ciudad de Victoria. Después, usó la información para disfrazarse de adolescente y crear un perfil convincente. Escrito por Luis Andrés Iregui. 16 marzo 2011.

1.10. Aporte Teórico

Todos los conceptos definidos en el proyecto serán un aporte para el entendimiento de los usuarios en general y las recomendaciones pertinentes en cada caso.

La novedad de la propuesta presentada consiste en la creación de una página Web, en la que por medio de videos, tutoriales, imágenes, orientará al usuario a que tome conciencia, propiciando una cultura de seguridad. Manteniendo la confidencialidad, integridad y disponibilidad de sus datos. Dicha página Web estará dirigida a adolescentes de 12 a 18 años.

1.11. Métodos de Investigación

El método de investigación que va a ser utilizado en este proyecto, es un método empírico haciendo uso de encuestas, muestreo, investigaciones entre otros.

2. Marco Contextual

2.1. Entorno del objeto de estudio

La Ingeniería Social es tan antigua como la humanidad, ya que desde tiempos inmemorables han existido timadores y embaucadores. Lo que trata de conseguir la Ingeniería Social, es que otra persona haga o diga lo que nosotros deseamos. Además, mucho antes del nacimiento de la red Internet ya se utilizaban esas técnicas con propósitos deshonestos y con excelentes resultados, aunque nadie las acuñó con el término de Ingeniería Social, eran conocidas con nombres como "El timo de la estampita", "El tocomocho", "El Nazareno", entre otros.

La Ingeniería Social se compone por tanto de técnicas de engaño de todo tipo, tanto en el mundo físico como en el virtual que, desgraciadamente, están muy de moda hoy en día, sobre todo en su faceta relacionada con las TIC (Tecnología de Información y Comunicación).

Actualmente, la Ingeniería Social es uno de los vectores de ataque más peligroso.

A esto se le debe sumar la popularidad de las redes sociales en Internet, que ha trascurrido en paralelo al aumento de los niveles de intercambio de contenidos a través de la Red. Esto ha hecho de Internet un medio más social que permite comunicar, entretener y compartir información, haciendo más fácil el trabajo de los ingenieros sociales.

Las redes sociales cuentan con un alto nivel de riesgo, dado que los usuarios exponen no sólo sus datos de contacto o información profesional, sino que se pueden exponer de manera pública las vivencias, gustos, ideología y experiencias. El usuario no toma conciencia real de que sus datos personales serán accesibles por cualquier persona y del valor que éstos pueden llegar a alcanzar en el mercado.

Por todo ello, y a pesar de que las redes sociales cuentan con una infinidad de beneficios para sus usuarios, éstos no deben obviar el hecho de que se tratan de herramientas públicas y accesibles para cualquier tipo de persona, con

independencia de que las intenciones con las que se accede sean negativas o ilícitas.

Es habitual que los usuarios de redes sociales no sean conscientes o descuiden la privacidad de sus perfiles. Así, en el reciente estudio *"Redes Sociales Análisis cuantitativo y cualitativo sobre hábitos, usos y actuaciones"* publicado por Ofcom (Office of Communications) en el cual se afirma que casi la mitad de los usuarios de redes sociales analizados (43%), tienen su perfil de usuario sin restricciones de privacidad y disponible para que pueda ser visitado por cualquier otro usuario.

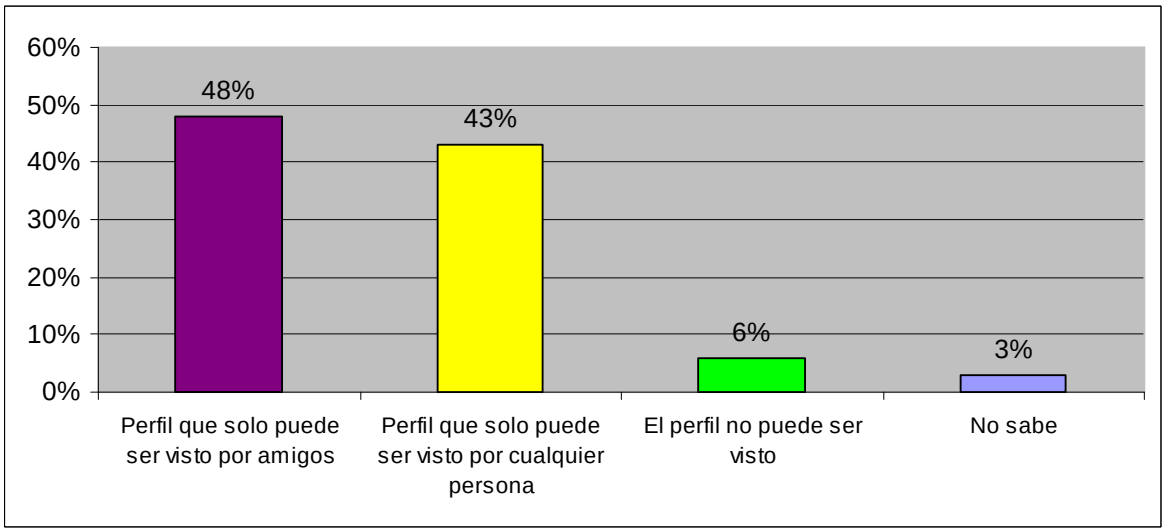


Ilustración 2- Perfil de los usuarios en las Redes Sociales.

Resumiendo, podemos apreciar que, la seguridad es un tema de nivel crítico teniendo en cuenta la inmensa cantidad de datos digitalizados y el continuo crecimiento de los mismos.

Además, debemos comprender que no hay tecnología capaz de proteger contra la Ingeniería Social, como tampoco hay usuarios ni expertos que estén a salvo de esta forma de ataque. *La Ingeniería Social no pasa de moda, se perfecciona y sólo tiene la imaginación como límite.*

2.2. Relación tesista y objeto de estudio

La idea principal del proyecto surgió al tener conocimiento de usuarios que

habían sido víctimas de algún tipo de engaño en Internet.

Al ahondar en el tema, desde una mirada de la Seguridad Informática, convergió en que todas estas formas de engañar al usuario, eran conocidas con el nombre de Ingeniería Social. Es por ello, que decidimos llevar adelante este Proyecto de Grado, enfocándonos en el usuario, eslabón más débil en la Seguridad Informática.

2.3. Análisis de los problemas observados

Cuando hablamos de Seguridad de la Información muchas veces nos olvidamos del usuario final, quien por lo general es el blanco de los delincuentes.

La gran cantidad de riesgos existentes en Internet, en las redes sociales y a esto sumado que la Ingeniería Social se ha convertido en uno de los métodos de ataque más frecuentes en nuestros días, es evidente lo expuesto que queda el usuario a estos peligros.

Se puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos, etc. Parece que está todo bajo control. Pero no es así, ya que los seres humanos, seres a los que *no se los puede configurar*, deben ser capaces y responsables de filtrar y eliminar las peticiones malintencionadas.

La capacidad del usuario de conocer y poder evitar ser víctima de engaños es menor a la velocidad con la que las técnicas de Ingeniería Social evolucionan. Esto genera la necesidad de introducir cambios que apunten a que los usuarios tomen conciencia y estén mejor preparados para reconocer y evitar rápidamente ataques de Ingeniería Social.

Sobre una población de 160 alumnos y 25 docentes del Colegio San José, localidad de San Agustín, las tesistas realizaron una encuesta. Alguno de los resultados se muestra a continuación.

En cuanto a los alumnos.

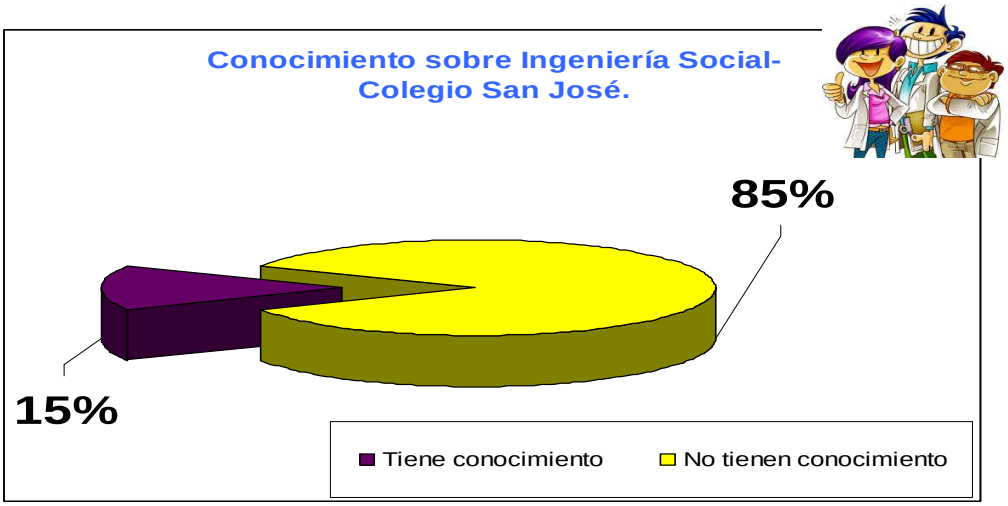


Ilustración 3- Porcentaje de alumnos con conocimiento de Ingeniería Social

Se puede apreciar que el 85 % de los alumnos de la Institución educativa no conoce o no ha escuchado hablar de la Ingeniería Social, mientras que el 15 % de los alumnos conoce sobre el tema.

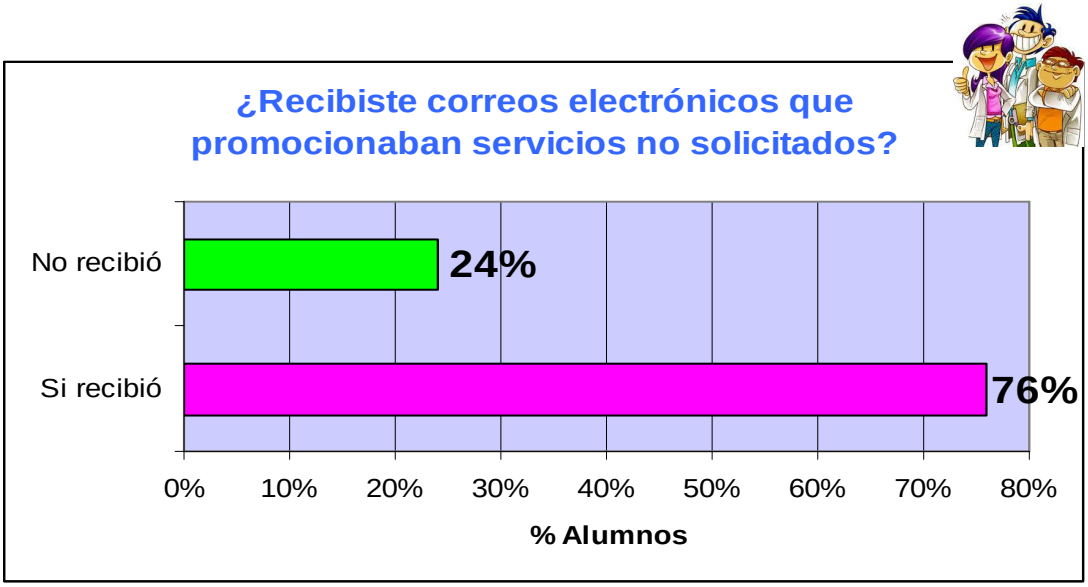


Ilustración 4- Porcentaje de recepción de correos electrónicos promocionando servicios no solicitados.

El 76 % de los alumnos han recibido correos electrónicos que promocionaban servicios no solicitados. De este porcentaje el 53 % de los alumnos visitó dichas páginas Web.

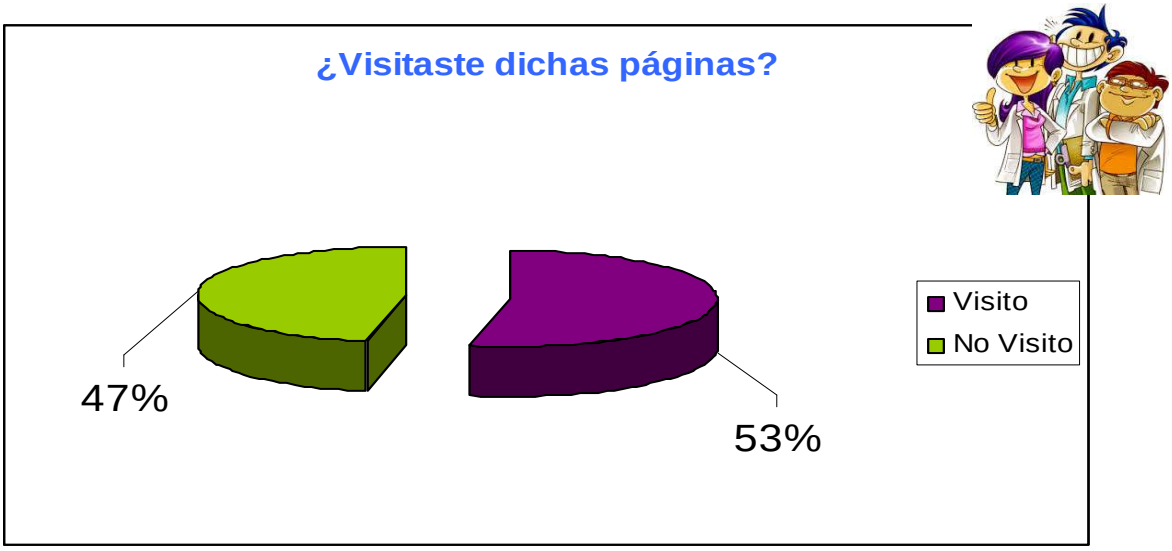


Ilustración 5- Porcentaje de visita de páginas que fueron enviadas por correo electrónico promocionando algún servicio no solicitado

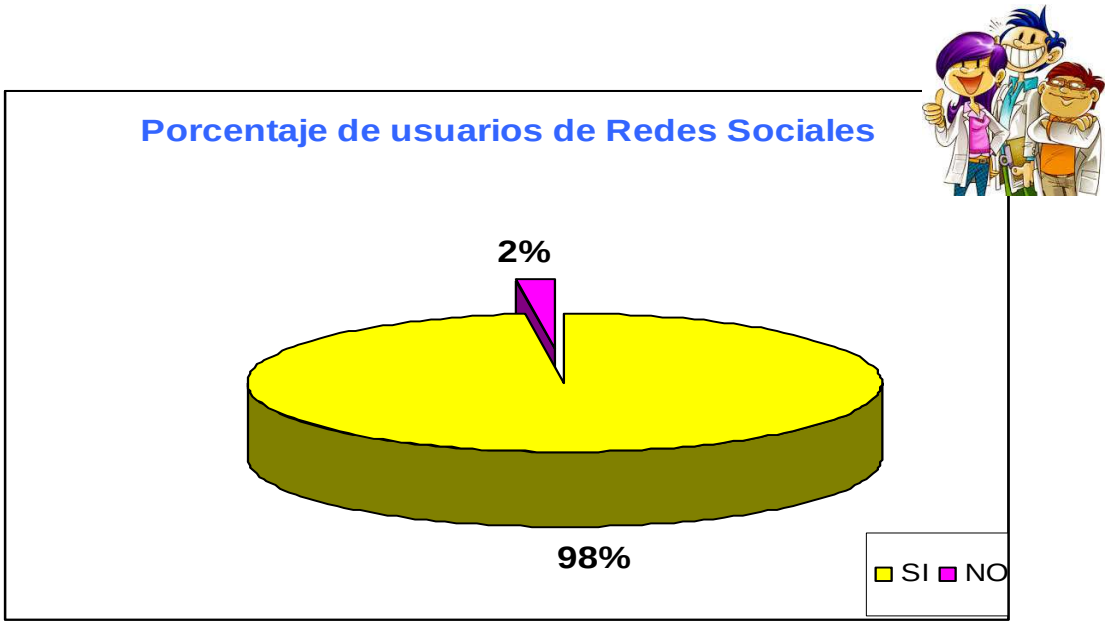


Ilustración 6- Porcentaje de usuarios de redes sociales.

El 98 % de los alumnos pertenece a alguna red social. Mientras que el 2 % no utiliza este servicio. Como se puede observar, es alto el porcentaje de usuarios de redes sociales.

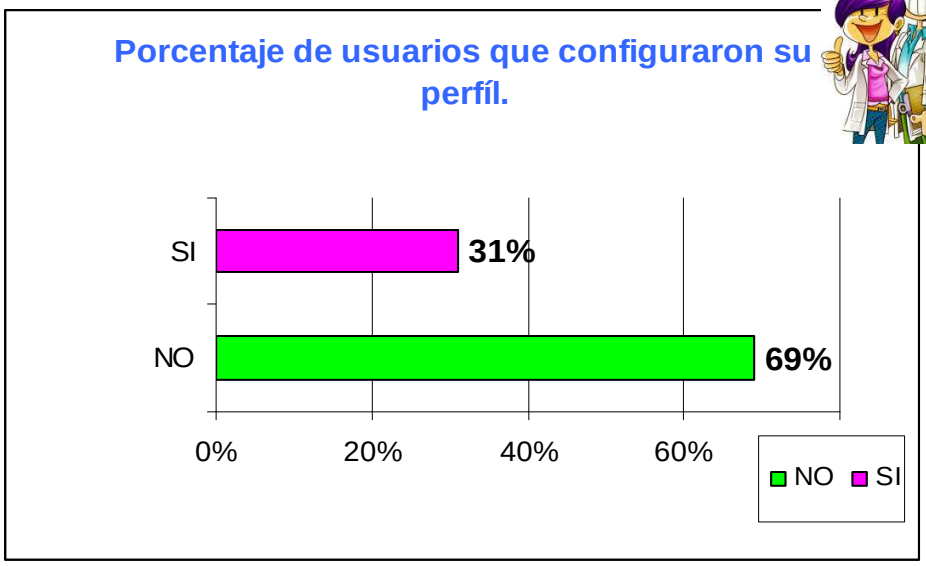


Ilustración 7- Porcentaje de usuarios que configuraron su perfil.

De los alumnos que utilizan redes sociales, sólo el 31% configuró su privacidad y seguridad en las redes sociales.

En cuanto a los docentes.

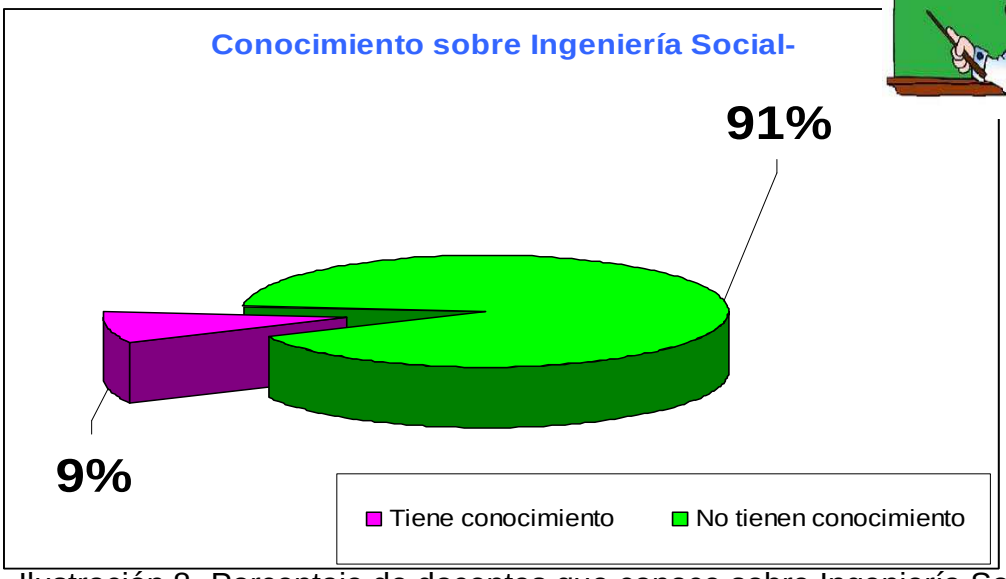


Ilustración 8- Porcentaje de docentes que conoce sobre Ingeniería Social

El 91 % de los docentes de la Institución educativa, no han escuchado hablar o no conocen lo que es la Ingeniería Social.

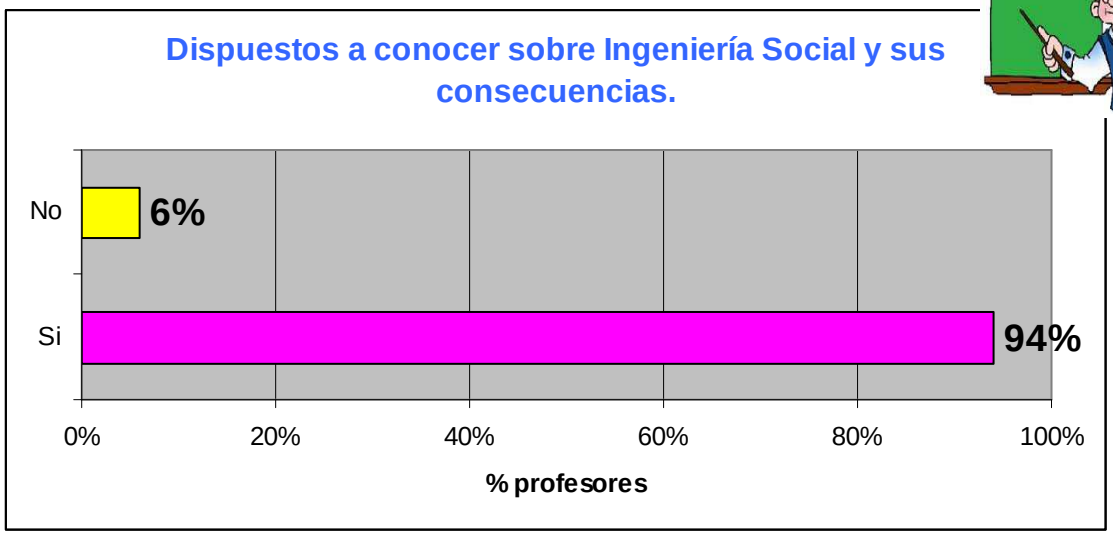


Ilustración 9- Porcentaje de docentes que esta dispuesto a conocer sobre el tema.

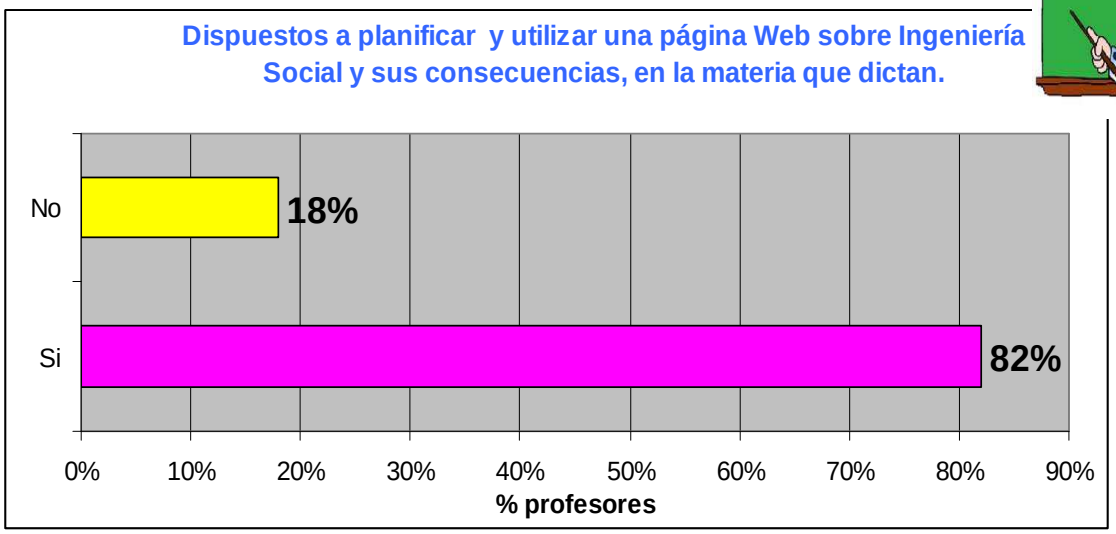


Ilustración 10- Porcentaje de docentes que esta dispuesto a realizar una intervención en su clase sobre el tema.

El 94 % de los docentes está dispuesto ha interiorizarse en el tema y el 82% a hacer una intervención en su clase. Se observó una gran disposición por parte de los docentes y del cuerpo directivo de la Institución.

Queda de manifiesto con estos porcentajes que los usuarios tienen una pobre conciencia acerca de la importancia de la seguridad. Es por ello que la principal defensa contra la Ingeniería Social es la educación de los usuarios. La mejor forma de combatir la Ingeniería Social es la prevención.

En el siguiente artículo, observamos lo vulnerable que es Facebook, una de las redes sociales más utilizadas por los alumnos.

Fuente: una publicación de Gastón Charkiewicz, el 4 de febrero de 2014 en Welivesecurity sita lo siguiente:

"10 años de Facebook a través de 10 acontecimientos de (in)seguridad"

"Hoy cumple 10 años Facebook, una de las redes sociales más populares de la actualidad. Dueña de políticas de privacidad que han dado que hablar más de una vez, cuenta con más de mil millones de usuarios y ha logrado mantenerse vigente a pesar del surgimiento de nuevas redes sociales. En su décimo cumpleaños queremos recordar 10 amenazas en lo que respecta a esta plataforma y su impacto en los usuarios.

Vulnerabilidades:

Facebook fue concebida como una red social para estudiantes universitarios donde podían compartir información acerca de sus gustos e intereses. Con el correr del tiempo logró difusión al punto de abrirse para todo tipo de usuarios, logrando además integraciones con servicios como iTunes y Youtube. Sin embargo, esta popularidad también la convirtió en objetivo de ataques y amenazas. Veamos algunas de ellas:

- *A principios del 2013, un investigador descubrió una vulnerabilidad en el restablecimiento de claves de usuario, que hacía posible que cualquiera pueda reestablecer una contraseña sin necesidad de conocer la original.*
- *En febrero de 2011, la red social anuncia su nuevo soporte para iframes. Si bien esto representó un avance para que desarrolladores pudieran utilizar*

nuevas funcionalidades, también conformó un nuevo vector de ataque, debido a que los iframes permiten la ejecución de contenido externo a la página sin necesidad de salir de la misma.

- *En diciembre de 2011 se detecta una vulnerabilidad en Facebook que permitía acceder sin autorización al contenido privado de cualquier usuario. La vulnerabilidad fue explotada para afectar a su Ceo,, Mark Zuckerberg.*

- *En febrero de 2013, los sistemas de la empresa se vieron infectados por un exploit 0-day de java.*

- *En junio de 2013 se dio a conocer que 6 millones de usuarios tuvieron su información expuesta durante un año.*

Amenazas de terceros

Los cibercriminales por lo general buscan difundir sus amenazas lo más posible. Por eso ¿qué mejor que una red social de más de mil millones de usuarios? Aquí presentamos 5 amenazas que a lo largo de los años han utilizado Facebook con éxito para propagarse:

- *A finales de 2009, se dieron a conocer ataques de phising a Facebook generados por Zeus, una de las botnets más populares y más grandes conocidas actualmente.*
- *En 2010, se conocieron unos hoax (mensajes falsos, distribuidos de forma masiva, con fines de molestar o causar miedo, por ejemplo) donde "aparentemente" el emisor era el fundador de Facebook.*

- *En 2011, una campaña que ofrecía averiguar quién visita tu perfil tuvo la finalidad de cambiar la página de inicio de los usuarios por la de un buscador que utilizaba el servicio de pago por clic de Google.*

- *Una aplicación de Facebook que simulaba verificar qué tan segura es una contraseña de correo, terminaba robando las credenciales de usuario de sus víctimas.*

- *Diversas campañas de "videos prohibidos de famosos" se han llevado a cabo con fines maliciosos, como el phishing que simulaba ser un video de Silvina Luna o el falso video de Justin Bieber que propaga malware.*

Como conclusión, podemos ver que con los años Facebook ha sido noticia por reiterados conflictos de seguridad. Sin embargo ha estado trabajando en solucionarlos y, de esa forma, ha mantenido su popularidad en su extenso ciclo de vida, que continua vigente hasta el día de hoy. Esta popularidad además ha hecho de la red social una de las elecciones más buscadas por los cibercriminales, que llevan a cabo sus campañas buscando masividad en ella. Es por eso que recomendamos su utilización de forma cuidadosa.

La popularización del uso de redes sociales asociado al desconocimiento de aplicación de controles de aseguramiento para las cuentas y perfil publicado, ofrecen para el proceso de obtención de datos un abanico de posibilidades de fuentes de información.

La forma más eficaz de protegerse frente a estas amenazas es mantenerse informado, saber cuáles son los peligros, qué se debe evitar y con qué hay que tener cuidado. Se apunta a que mayor cantidad de personas puedan conocer más acerca de la Ingeniería Social y Seguridad Informática y, de esta forma, hagan un buen uso de las nuevas tecnologías de la comunicación.

2.4. Antecedentes de proyectos similares

El antecedente que se presenta a continuación es un informe que habla sobre el fraude a través de Internet, utilizando técnicas de Ingeniería Social.

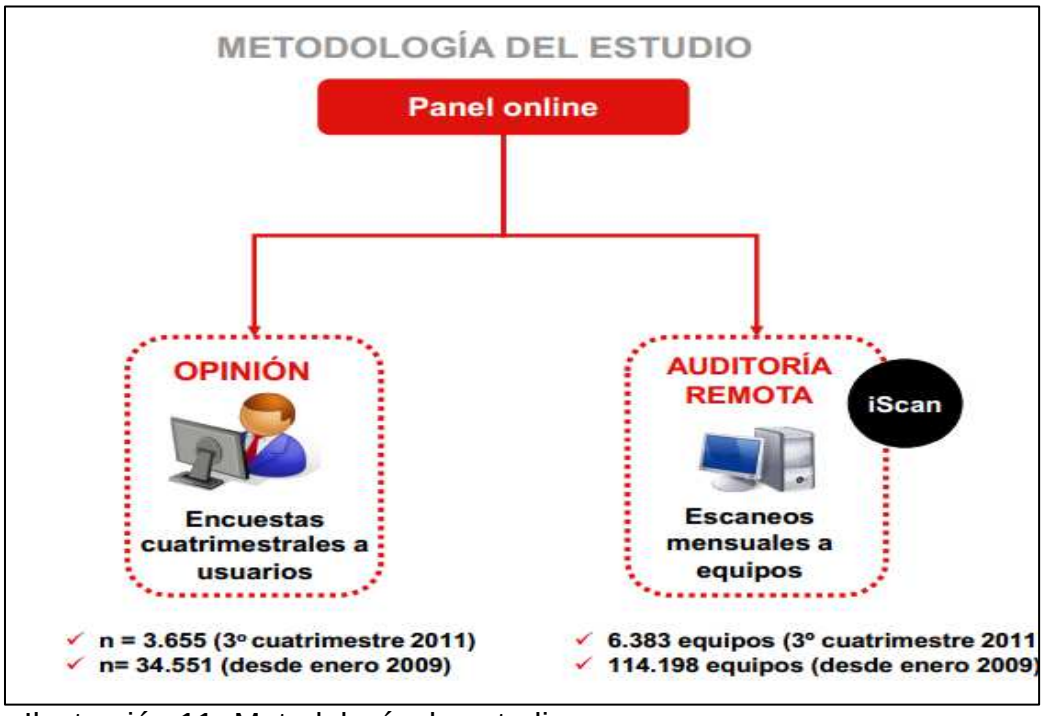
"La metodología utilizada para la realización del informe combina entrevistas a usuarios de Internet y escaneo online de equipos de hogares. Además, ofrece un análisis evolutivo del año 2011, haciendo una comparativa con los datos de 2009 y 2010.

El informe permite realizar un diagnóstico de la incidencia de situaciones que podrían crear intentos de fraude entre los usuarios de Internet. Asimismo,

analiza el impacto que estas situaciones han tenido a nivel económico y la influencia que han ejercido en los hábitos relacionados con la banca a través de Internet y el comercio electrónico. El estudio muestra también las diferencias existentes entre los usuarios que han sufrido intento de fraude y los que no, a la hora de depositar su confianza en la realización de operaciones bancarias a través de Internet y compras online.

OBJETIVOS DEL ESTUDIO

- Estudiar los intentos de fraude que han afectado a los encuestados.
- Caracterizar las diferentes formas de fraude recibido y sus métodos de distribución.
- Analizar el impacto económico del fraude a nivel particular.
- Identificar las diferentes familias de malware que les afectan.
- Ponderar el nivel de confianza de los usuarios y orientarle en las diferentes medidas de seguridad utilizadas tras los ataques de fraude.



. Ilustración 11- Metodología de estudio

Ficha técnica

Universo
Usuarios de Internet mayores de 15 años con acceso frecuente a Internet desde el hogar.

Muestra
3.655 usuarios encuestados.
6.383 análisis remotos.

Distribución muestral
Muestreo polietápico con estratificación por Comunidades Autónomas y cuotas de tamaño por hogar, edad, sexo, actividad laboral y tamaño del hábitat.

Captura de información
Entrevistas online. Análisis en línea de los equipos.

Trabajo de campo
Septiembre a diciembre de 2011.

Error muestral
De acuerdo con los criterios del muestreo aleatorio simple para variables dicotómicas en las que p=q=0,5 y para un nivel de confianza del 95,5%, se establece un error muestral de ±1,62% para n= 3.655.

Intento de fraude y manifestaciones

- Un 58,4% de los internautas declara haber sufrido algún intento de fraude (no necesariamente consumado) a través de la Red en los últimos 3 meses.
- La recepción de correos electrónicos invitando a visitar páginas Web sospechosas (43,3%) o promocionando servicios no solicitados (32,7%) son las situaciones más frecuentes.

Forma adoptada por el remitente origen de la comunicación sospechosa de ser fraudulenta

- Los principales formatos utilizados en los mensajes con apariencia sospechosa son las Web de comercio electrónico y las entidades bancarias (ambas con un 39,8%), seguidas de las loterías (30,8%).
- Otras opciones, como los particulares y las redes sociales experimentan notables incrementos desde 2009.

Impacto económico del fraude

- La incidencia de fraude a través de Internet con impacto económico se mantiene estable desde 2009. A finales de 2011 alcanza el 3,4%.
- La cuantía defraudada es inferior a 400€ en la mayoría de las ocasiones (un 93,3%). Desde 2009 se producido un aumento progresivo de los fraudes de pequeña cuantía.

Fraude y malware

- En diciembre de 2011, un 36,5% de los equipos analizados aloja algún tipo de troyano, un 5,7% troyanos bancarios y un 4,6%, rogueware.
- La proporción de equipos infectados a finales de 2011 es levemente superior a la de 2009 en el caso de los troyanos genéricos e inferior en el de los troyanos bancarios y el rogueware.

Influencia en los hábitos relacionados con la banca a través de Internet y el comercio electrónico

- Existe un notable nivel de confianza en la realización de operaciones bancarias y compras con tarjeta en Internet, con independencia de haber sufrido una pérdida económica a consecuencia de un intento de fraude.
- A pesar de haber sufrido un intento de fraude, 3 de cada 4 internautas no modifican sus hábitos de comercio electrónico o banca online.

A continuación un resumen de porcentajes de tendencias sobre el fraude a través de Internet.

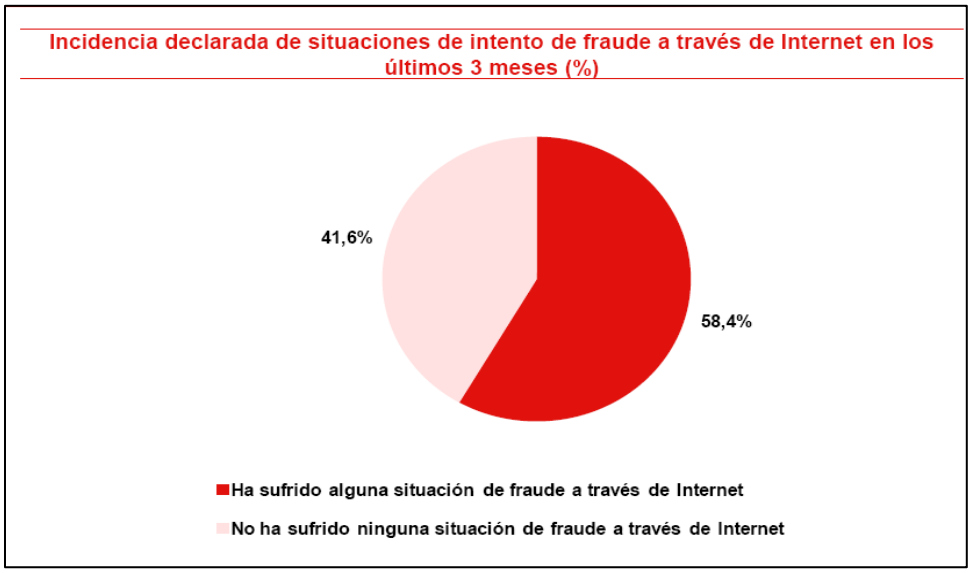


Ilustración 12- Porcentaje de Incidencia de situaciones de intento de fraude

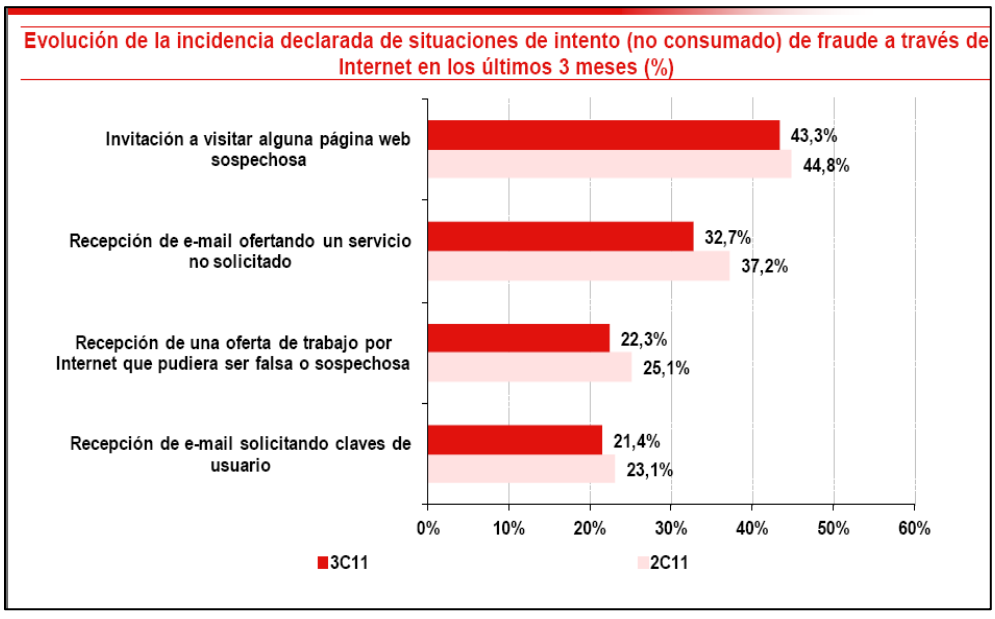


Ilustración 13- Porcentaje de Incidencia de situaciones de intento de fraude no consumado.

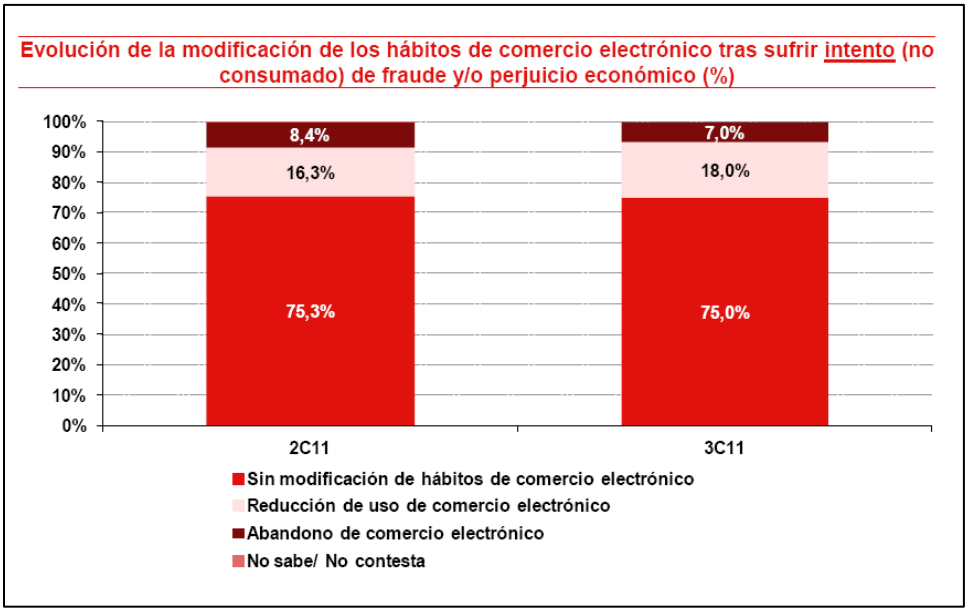


Ilustración 14- Porcentaje de evolución de hábitos de comercio electrónico.

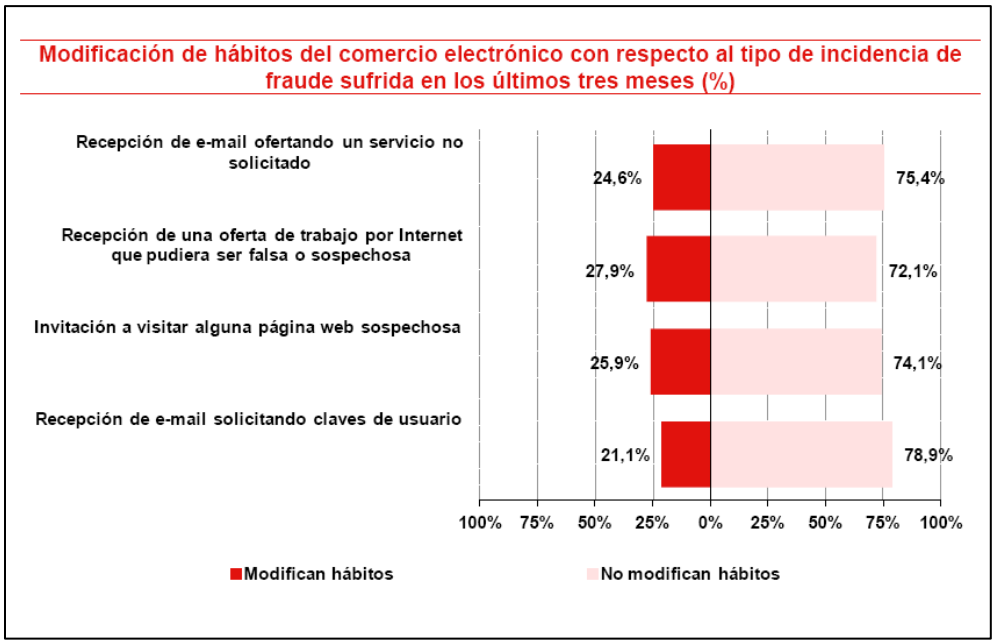


Ilustración 15- Porcentaje de influencia en los hábitos relacionados con la banca a través de Internet y el comercio electrónico.

En conclusión:

- La industria de seguridad ha caracterizado al 2011 como el año de los ciber ataques dirigidos a multitud de sectores. Tanto el malware como los mecanismos de Ingeniería Social son perfeccionados para lograr el máximo impacto.
- Los resultados obtenidos por INTECO muestran que crece la proporción de intentos (no necesariamente consumados) de fraude a través de Internet. Por tanto, el fraude online avanza con respecto a años anteriores.

- En 2011, los internautas detectan más mensajes que simulan proceder de supuestas redes sociales y de particulares, fórmulas que se unen a las tradicionales (comercio electrónico, banca y páginas de loterías).

- El fraude de pequeñas cantidades es el que más afecta a los hogares, desde 2009 ha aumentado la proporción de fraudes reportados.

- En todo caso, los usuarios siguen mostrándose fieles a la compra y banca online y no retiran su confianza incluso tras haber vivido una situación de fraude. Resulta positivo que cada vez son menos los que muestran una actitud pasiva y más los que adoptan opciones diferentes al abandono de servicios de banca online o comercio electrónico.

3. Marco Teórico

3.1. Conceptos de la Seguridad Informática

Objetivo de la Seguridad Informática

La Seguridad Informática busca dar apoyo a los objetivos y misión de las organizaciones, a través de la protección de sus principales recursos y activos como son: la información, la tecnología que la soporta (hardware y software) y las personas que la utilizan o conocen, a través de la selección y aplicación de protecciones adecuadas, cuidando de esta manera, sus recursos físicos, financieros, reputación, y otros activos tangibles e intangibles.

La Seguridad Informática ha definido tres principios básicos que son: *confidencialidad, integridad y disponibilidad* y, cuatro servicios: *autenticación, autorización, no repudio y auditabilidad* para poder cumplir su objetivo.

Principios de la Seguridad Informática

La correcta Gestión de la Seguridad de la Información busca conservar la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no estamos ante nada seguro. Hay que conocer siempre las vulnerabilidades y las amenazas que se pueden producir sobre cualquier información, teniendo en cuenta las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener.

Uno de los objetivos principales de la Seguridad Informática, es mantenerlos seguros frente a las diversas amenazas a las que se enfrentan y que pueden afectar su funcionalidad de diferentes maneras: corrupción, acceso indebido e incluso hurto y eliminación.

La Seguridad Informática se basa en la preservación de unos principios básicos, que se definen a continuación:

- **Confidencialidad**.

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Este principio tiene como propósito asegurar que sólo la persona o personas autorizadas tengan acceso a cierta información. Esto significa que se debe asegurar que las personas no autorizadas, no tengan acceso a la información restringida para ellos.

- **Integridad.**

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

La integridad tiene como propósito principal, garantizar que la información no sea modificada o alterada en su contenido por sujetos no autorizados o de forma indebida.

Asimismo, la integridad se aplica a los sistemas, teniendo como propósito garantizar la exactitud y confiabilidad de los mismos.

- **Disponibilidad.**

Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

Este principio tiene como propósito, asegurar que la información y los sistemas que la soportan, estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos. Al referirse a los sistemas que soportan la información, se trata de toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento de la información.

En conclusión, disponibilidad, integridad y confidencialidad son principios

básicos de la Seguridad Informática, y su adecuada comprensión es necesaria en esta investigación, para la correcta identificación de problemas y las soluciones apropiadas a ellos.

Servicios de la Seguridad Informática

Para lograr hacer cumplir la preservación y el cumplimiento de los tres principios básicos de la Seguridad Informática, se han planteado cuatro servicios principales.

- **Autenticación.**

Busca asegurar la validez de una identificación proporcionada para acceder a cierta información, proveyendo medios para verificar la identidad de un sujeto.

- **Autorización.**

Permite la especificación y continua administración de las acciones permitidas por ciertos sujetos, para el acceso, modificación o inserción de información de un sistema, principalmente, mediante permisos de acceso sobre los mismos.

- **No Repudio.**

La administración de un sistema de información debe estar en capacidad de asegurar quién o quiénes son los remitentes y destinatarios de cualquier información. Proveer los medios y mecanismos para poder identificar quien ha llevado a cabo una o varias acciones en un sistema, para que los usuarios no puedan negar las responsabilidades de las acciones que han llevado a cabo.

- **Auditabilidad.**

Proporciona los mecanismos para la detección y recuperación ante posibles fallas o incidentes de seguridad, mediante el registro de todos los eventos y acciones hechas en un sistema.

Administración de la Seguridad Informática

Actualmente se escucha en varios medios acerca de incidentes de Seguridad Informática, como ataques que causan pérdidas y daños que pueden llegar a representar grandes sumas de dinero para una organización, ataques remotos a instituciones financieras, ataques a los sitios Web de grandes y prestigiosas empresas y corporaciones, etc.

Este tipo de incidentes son los que hacen cada vez más interesante la Seguridad Informática, pero así mismo, significa tareas y responsabilidades diarias de ésta área para prevenir ataques como los antes mencionados.

Seguridad de la información

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos de saber que puede ser confidencial. La información está centralizada y puede tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Esto afecta su disponibilidad y la pone en riesgo.

La información es poder y a la información se le conoce como:

- Critica: Es indispensable para la operación de la empresa.
- Valiosa: Es un activo de la empresa y muy valioso.
- Sensitiva: Debe de ser conocida por las personas autorizadas.

3.2. Conceptos de Ingeniería Social

Ilustración 16- Ejemplificación de Ingeniería Social.

La *Ingeniería Social* es un conjunto de técnicas psicológicas y habilidades sociales (como la influencia, la persuasión y sugestión) implementadas hacia un usuario directa o indirectamente para lograr que éste revele información sensible o datos útiles sin estar conscientes de su maliciosa utilización eventual. Estas pueden estar llevadas a cabo mediante el trabajo con tecnología y ordenadores o directamente a través del trato personal. El objetivo es evadir o hacer más fácil el acceso a los sistemas de seguridad tradicionales al acceder a la información desde la fuente más confiable pero más vulnerable, el propio protegido.

Wikipedia define Ingeniería Social como: " es el acto de manipular a la gente a realizar acciones o divulgar información confidencial. Mientras que es similar a una estafa o fraude simple, el término se aplica generalmente a engaño o engaño con fines de recolección de información. En la mayoría de los casos, el atacante no se encuentra cara a cara con la víctima". La Ingeniería Social en realidad toca muchos aspectos de la vida diaria. Muchos consideran que la Ingeniería Social es el mayor riesgo para la seguridad.

En el campo de la Seguridad Informática, la Ingeniería Social se conoce como la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Asimismo, se la define como aquellas conductas y técnicas utilizadas para conseguir información de las personas. Por otro lado, es también una disciplina que consiste en sacarle información a otra persona sin que ésta se

de cuenta de que está revelando información sensible y que normalmente no lo haría bajo otras circunstancias. La Ingeniería Social se sustenta en el principio de que en cualquier sistema "los usuarios son el eslabón más débil", así lo define la Dra. Aury Curbelo, especialista en Seguridad Informática.

El inicio de la Ingeniería Social se remonta a Kevin Mitnick, quien evadió a la justicia durante casi veinte años antes de ser detenido, por realizar diferentes delitos del orden público, falsificando y sustrayendo datos e información confidencial de varias universidades y departamentos del estado.

Kevin Mitnick, comentó que "La gente por no querer quedar mal o crear un escándalo, brinda a cualquiera que le solicita, información sensible, y ahí es donde juega un papel importante la educación, el enseñarle a los usuarios a decir no".

La mayoría de las técnicas tienen una base de influencia social, a través de la observación del comportamiento humano. Kevin Mitnick define una metodología que consta de cuatro etapas que se muestra a continuación.

Ciclo de vida de la Ingeniería Social	
ACCIÓN	**DESCRIPCIÓN**
Investigación	Se investiga en fuentes abiertas de información, como informes anuales, material de marketing, contenidos en Internet, remover la basura, etc.
Desarrollar rapport y credibilidad	Se usa la información interna, se reemplazan identidades, se reclama a la víctima, se le pide ayuda, o se usa la autoridad.
Explotar confianza	Se pregunta o se consigue que te pregunten con el fin de conseguir el objetivo marcado.
Utilizar información	Si la información es sólo una parte, se vuelve a empezar el ciclo, hasta conseguir el objetivo.

El ciclo es simple, pero no por ello poco eficaz. Se puede resumir en buscar información, crear confianza y utilizarla. Además, siempre se produce en el mismo escenario, en el que encontramos:

- Atacante: es una persona quien debe preparar y ejecutar la acción.
- Medio: es la vía por la que se produce la comunicación.
- Víctima: es una persona manipulada que ejecuta la voluntad del atacante sin conocimiento de causa.
- Pretexto: es la historia que se crea y se argumenta por tal de convencer a la víctima.

A continuación se detalla lo antes descripto.

- **Identificar a la Víctima**. En esta área se comprende la psicología de la víctima, y de ser necesario, el ingeniero social se convierte en una persona totalmente distinta a fin de agradarle y obtener la información que desea.

- **Reconocimiento**. No es otra cosa que obtener información de la víctima.
    a. Ahora bien, ¿dónde obtenemos información de la víctima? La obtención de información se puede realizar mediante sitios Web, bases de datos, grupos de noticias, socios de negocios, “dumpster diving” búsqueda en la basura.
    b. Existe una herramienta que es una de las más poderosas hoy en día y es la red social Facebook. Al visitar los perfiles de Facebook, uno puede darse cuenta que la mayoría de las personas no se toman la molestia de manejar su perfil como privado, por el contrario, lo dejan como público. Gracias a estos muros de datos personales encontramos información como nombre, fecha de nacimiento, lugar de nacimiento, escuelas donde estudió, empresas en las que ha trabajado, amistades e incluso fotografías.

c. Telefónicamente, el atacante se hace pasar por otra persona o sorprende en su buena fe al usuario aprovechándose de su ignorancia o inocencia, y así consigue información importante.
d. Investigando en los contenedores de basura de la víctima. Allí pueden encontrarse datos útiles como horarios de vigilancia, nombres y códigos de empleados, procedimientos de la empresa, códigos fuente, discos u otros dispositivos de almacenamiento.

- **Crear el escenario.** Una vez estudiado cuidadosamente quién es la víctima, se procede a crear un escenario creíble en el cual participarán la víctima y el ingeniero social. La parte más importante de un ataque es la creación del escenario que dará pie al ataque en sí. Este escenario apela a todos los principios antes expuestos y cuidadosamente elaborados para engañar a la víctima. Puede ser una situación por teléfono, una aparición física al área de trabajo, a través de Internet, entre otras, en fin existen diversos medios para crear el escenario del ataque.

- **Realizar el ataque.** Por supuesto la realización del ataque supone que se conocen de ante mano toda la información necesaria para llevarlo a cabo sin dejar rastros.

- **Obtener la información.** Una vez que se obtiene la información deseada solo procede a salir.

- **Salir.** Finalmente el salir implica el borrado de huellas, de modo que no queden evidencias de que se estuvo allí.

A continuación hablaremos de los principales elementos que facilitan a los atacantes el robo de información. Como veremos, la gran mayoría de estos no son de carácter técnico sino humano. *"Es hora de activar el Antivirus mental".*

Los principios de la Ingeniería Social están basados en el aspecto psicológico de los seres humanos. Kevin Mitnick fundamenta las estrategias de Ingeniería Social en los siguientes postulados.

- Todos los seres humanos quieren ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir NO.
- A todos nos gusta que nos alaben.
- Todos tenemos algo de ingenuos.

Desde el punto de vista de la psicología humana, existen determinados procesos que son automáticos en el ser humano en virtud de las relaciones con los demás. Así que depende de quién lo analice, y los convierta en una ventaja o una desventaja para obtener información. Estos procesos son comúnmente utilizados en campañas de mercadeo y negocios para influenciar sobre la gente.

Otras estrategias o principios de la Ingeniería Social se basan en rutas periféricas de persuasión en donde se utiliza la emoción como una forma de distracción. Entre los destacados investigadores en el área de persuasión se encuentra el Dr. Robert Cialdini.

El Dr. Cialdini es un profesor de la Universidad Estatal de Arizona y su investigación académica se centra mayormente en porqué la gente a menudo cumple con peticiones sin realmente pensar acerca de sus necesidades. Dr. Cialdini en su libro sobre la persuasión, definió seis armas de influencia:

- **Reciprocidad**: Por norma general la gente tiende a devolver un favor. Cicerón decía: “No hay deber más obligatorio que la devolución de los favores”. Asimismo, la reciprocidad es un principio muy poderoso.
- **Compromiso y consistencia:** Se define cuando una persona se compromete a llevar a cabo lo que ha decidido que es correcto. Cuando un atacante o ingeniero social logra comprometer a su víctima ésta no le quedará más remedio que ceder ante las presiones del atacante.

- **La prueba social**: Las personas harán aquellas cosas que vean que otras personas hacen. Es la tendencia a imitar a los semejantes.
- **Autoridad**: Es una de las más explotadas por los ingenieros sociales. La gente tiende a obedecer a figuras con autoridad, que se destaquen en su ámbito. Lo que facilita al ingeniero social identificar quién es la autoridad en la empresa y hacerse pasar por él o ella.
- **El Gusto:** Toma en cuenta el principio de que las personas son convencidas fácilmente por otra persona con quien se sienten a gusto. Generalmente, las personas con buena presencia van a tener más facilidad de influir a otros.
- **La Escasez:** Tendencia a valorar más lo que es escaso. Aquí el ingeniero social toma en cuenta que la escasez percibida generará la demanda. Por eso al crear un correo electrónico falso con ofertas falsas, existe una gran probabilidad de que los usuarios se vean tentados a abrirlos y por lo tanto se descarga un "malware" o troyano en su ordenador que abrirá una puerta trasera al atacante y le permitirá entrar en la red de la empresa u hogar.

¿Por qué la Ingeniería Social es tan efectiva?

Existen cientos de razones que podrían explicar por qué la Ingeniería Social es tan efectiva, sin embargo se mencionarán algunas de ellas.

- **El campo de la seguridad de la información está enfocado principalmente en seguridad técnica**. Todas las empresas se han enfocado en crear muros de fortalezas con la mejor tecnología, protegiendo así todos sus activos con los mejores "firewalls", todas las actualizaciones al día, con políticas de seguridad (todas ellas enfocadas en aspectos técnicos), en fin todo lo que tiene que ver con la fase técnica de un sistema de información. Ahora bien, es poco lo que presupuestan para atender las necesidades de orientación y capacitación en áreas relacionadas al aspecto humano de esa cadena de protección de datos.

- **Casi no se presta atención a la interacción máquina-persona**. Mucho se ha estudiado y reportado sobre la importancia de atender la interacción máquina-persona, sin embargo, muy pocas empresas entienden que reforzando el lado humano mediante adiestramientos y seminarios acerca de la Ingeniería Social se crea una cultura de seguridad que a la larga se convierte en un retorno de inversión.

- **Ingeniería Social es extremadamente difícil de detectar**. No existe un sistema de detección de intrusos para detectar la "falta de sentido común" o ignorancia del usuario.

En la actualidad, la Ingeniería Social es quizá la técnica más divulgada para propagar ciberataques, porque consiste en la utilización o aprovechamiento de las debilidades en los usuarios, utilizando su desconocimiento o miedo, entre otros factores, para aprovecharse de su ingenuidad y obtener lo que queremos. En este caso: acceso a la información.

El perfil del Ingeniero Social

Las cualidades que debe poseer un ingeniero social para destacarse en esta disciplina pueden ser varias, desde su habilidad para relacionarse con sus pares hasta cuales son sus ambiciones, conocimientos en el área de informática, su apariencia de inocencia, su credibilidad y su grado de curiosidad.

Las destrezas de un ingeniero social se pueden enseñar, practicar y dominar al punto de que Usted, con un poco de adiestramiento y gran capacidad para convencer, puede convertirse en un ingeniero social en cuestión de meses.

Ahora bien, algunas de las características o requisitos más importantes, se destacan las siguientes:

- Capacidad de socializar con facilidad.
- Habilidad en el hablar.
- Habilidad en el arte de persuasión.

- Sonar convincente.
- Aparentar ser inofensivo.
- Mantener un perfil bajo.
- Sonreír siempre.
- Tono de voz cómodo.

¿Por qué caen las personas en estas trampas?

Las personas son víctimas de ataques de Ingeniería Social por varias causas, entre ellas;

- **Total desconocimiento del tema.** No se puede reconocer un ataque de Ingeniería Social, porque ni siquiera se reconoce el término, mucho menos se podrá identificar quién es un ingeniero social y porqué se hacen las preguntas para obtener información.
- **Falta de adiestramientos.** Es la variable más común en la lucha por la prevención e identificación de ataques de Ingeniería Social. Si no se capacita a la fuerza laboral sobre estos temas, las empresas seguirán siendo víctimas de estos ataques.
- **Actitud: "A mí no me va a pasar".** Esta actitud refleja la negación de muchas empresas a invertir en adiestramientos y en contramedidas para atacar la Ingeniería Social en el área laboral. Esta negación a capacitar al personal no técnico así como al técnico se ha traducido en cientos de miles de pérdidas anuales por la fuga de información.

3.2. 1. Técnicas de engaño utilizando Ingeniería Social.

Muchas de las técnicas utilizadas para conseguir información de forma ilegal contemplan la utilización de mecanismos, herramientas, equipos y la mayoría de las veces quienes las ejecutan necesitan de sofisticados conocimientos técnicos y amplia experiencia para que los ataques sean efectivos; sin embargo, la Ingeniería Social omite el dominio de cuestiones técnicas y se

basa en el aprovechamiento del *eslabón más débil* dentro de la Seguridad Informática, el usuario.

Mientras las nuevas tecnologías de comunicaciones han permitido que la brecha entre usuarios y máquinas sea cada vez menor, los complejos sistemas de comunicación también han desarrollado modelos que dan al usuario la capacidad de intercambiar información de una manera cada vez más rápida, fácil y sencilla. Ejemplos de esto es la evolución de los mensajes de correo electrónico, mensajeros instantáneos, redes sociales, mensajes de texto, etc., los cuales proporcionan una manera efectiva de intercambio de información.

El uso y aprovechamiento de tecnologías de este tipo, conllevan a que el usuario confíe en todo lo que hay detrás; es decir, si el usuario ve una interfaz amigable o conocida, normalmente supondrá que el emisor de dicha información es precisamente quien la está publicando.

En base a lo anterior se puede entender o al menos imaginar gran cantidad de formas por las cuales pueden aplicarse técnicas de engaño en medios como el correo electrónico, mensajes de texto, páginas Web, etc., de modo que los usuarios *ingenuos* proporcionen información o realicen acciones que deliberadamente han sido planeadas para lograr objetivos como robo de información, acceso a cuentas de usuario, etc.

A continuación desarrollaremos las técnicas más usadas para realizar Ingeniería Social.

Phising

Ilustración 17- Phishing

Es un tipo de estafa cuyo objetivo es el de intentar obtener los datos personales, claves, cuentas bancarias, números de tarjeta de crédito, identidades de una persona (usuario). Es una manera de pescar víctimas incautas a través de señuelos.

El estafador, conocido como phisher, se vale de técnicas de Ingeniería Social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales, llamadas telefónicas, duplicado de una Web idéntica a la entidad a la que quiere suplantar.

Los correos de tipo phishing generalmente contienen algún enlace a una página falsa que suplanta la identidad de una empresa o servicio en la que, si introducimos nuestros datos, éstos pasarán directamente a manos del estafador.

Cuando hablamos de phishing casi siempre lo relacionamos con el correo electrónico, aunque cada vez más, se están detectando casos de este fraude con el mismo objetivo, pero que redirigen a una página Web falsa a través de otros medios como pueden ser los mensajes intercambiados a través de aplicaciones de mensajería instantánea, mensajes en redes sociales o SMS.

De hecho, Kevin Mitnick se hizo famoso por su Phishing telefónico, con el cual pudo obtener información sensible de numerosos usuarios, mediante llamadas telefónicas.

¿Qué características tienen en común los correos de phishing?

Los mensajes suplantadores utilizan todo tipo de argumentos ingeniosos relacionados con la seguridad de la entidad o el adelanto de algún trámite administrativo para justificar la necesidad de facilitar sus datos personales. Entre las excusas frecuentes encontramos:

- Problemas de carácter técnico.
- Recientes detecciones de fraude y urgente incremento del nivel de seguridad.
- Nuevas recomendaciones de seguridad para prevención del fraude.
- Cambios en la política de seguridad de la entidad.
- Promoción de nuevos productos.
- Premios, regalos o ingresos económicos inesperados.
- Accesos o usos anómalos a tu cuenta.

- Inminente desactivación del servicio.
- Falsas ofertas de empleo.

Además, el correo fraudulento tratará de forzar al usuario a tomar una decisión de forma casi inmediata advirtiendo de consecuencias negativas, como por ejemplo la denegación de acceso al servicio correspondiente o el pago de una multa económica.

Aunque los timadores perfeccionan sus técnicas continuamente, los mensajes fraudulentos generalmente se generan a través de herramientas automáticas que integran funcionalidades de traducción y diccionarios de sinónimos por lo que suelen presentar faltas ortográficas y errores gramaticales.

¿Qué servicios son los más utilizados por los ciberdelincuentes para suplantar su identidad?

1. Bancos y cajas

Excusas utilizadas para engañar al usuario: Cambio en la normativa del banco, cierre incorrecto de la sesión del usuario, mejoras en las medidas de seguridad, detectada intrusión en sus sistemas de seguridad, bloqueo de la cuenta por motivos de seguridad, etc.

Objetivo: Robar números de tarjetas de crédito, tarjetas de coordenadas, PIN secreto, etc.

Algunos ejemplos: Pghishing al Banco Santander, al Banco BBVA. Standard Bank.

Ilustración 18- Ejemplo de phishing bancario.

2. Pasarelas de pago online (MasterCard, Visa, otras)

Excusas utilizadas para engañar al usuario: Cambio en la normativa del servicio, cierre incorrecto de la sesión del usuario, mejoras en las medidas de seguridad, detectada intrusión en sus sistemas de seguridad, etc.

Objetivo: Robar datos bancarios.

Ejemplos: Phishing a MasterCard.

Se ha detectado una campaña masiva de phishing, 5942 mails, que corresponde a una falsa notificación de actualización del reglamento de la UE para la utilización de tarjetas de crédito.

Los correos electrónicos tienen el siguiente aspecto:

Ilustración 19- Ejemplo de phishing a Master Card.

Todos los mails contienen un fichero adjunto de nombre **Actualization.zip**, que una vez descomprimido y ejecutado su contenido muestra la siguiente pantalla:

Ilustración 20- Fichero adjunto al mail de Campaña masiva de MasterCard.

Si el usuario se cree el mensaje, cumplimenta el formulario con sus datos bancarios y pulsa el botón de "Completar", estos datos acabarán almacenados en servidores controlados por atacantes.

3. Redes sociales (Facebook, Twitter, Instagram, Linkedin, etc.)

Excusas utilizadas para engañar al usuario: alguien te ha enviado un mensaje privado, se han detectado conexiones extrañas en la cuenta, por motivos de seguridad es necesario que se cambien las claves, etc.

Objetivo: Robar cuentas de usuarios, obtener sus datos privados y suplantar su identidad.

Ejemplos: Phishing en Facebook, en Twiter.

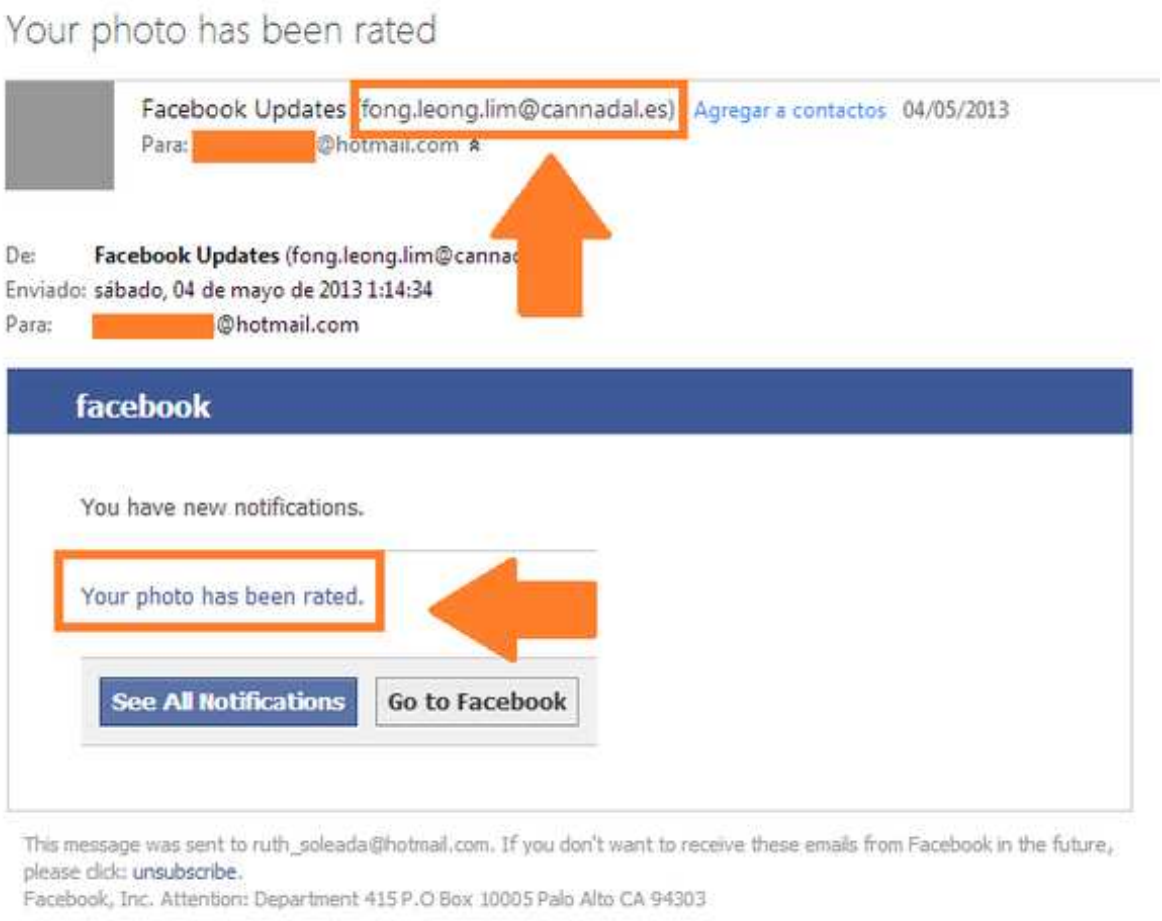


Ilustración 21- Phishing a Facebook.

4. Páginas de compra/venta y subastas (Amazon, eBay, etc.)

Excusas utilizadas para engañar al usuario: Problemas en la cuenta del usuario, se detectaron movimientos sospechosos, actualización de las condiciones del uso del servicio, etc.

Objetivo: Robar cuentas de usuarios y estafarlo económicamente.

Ejemplos:

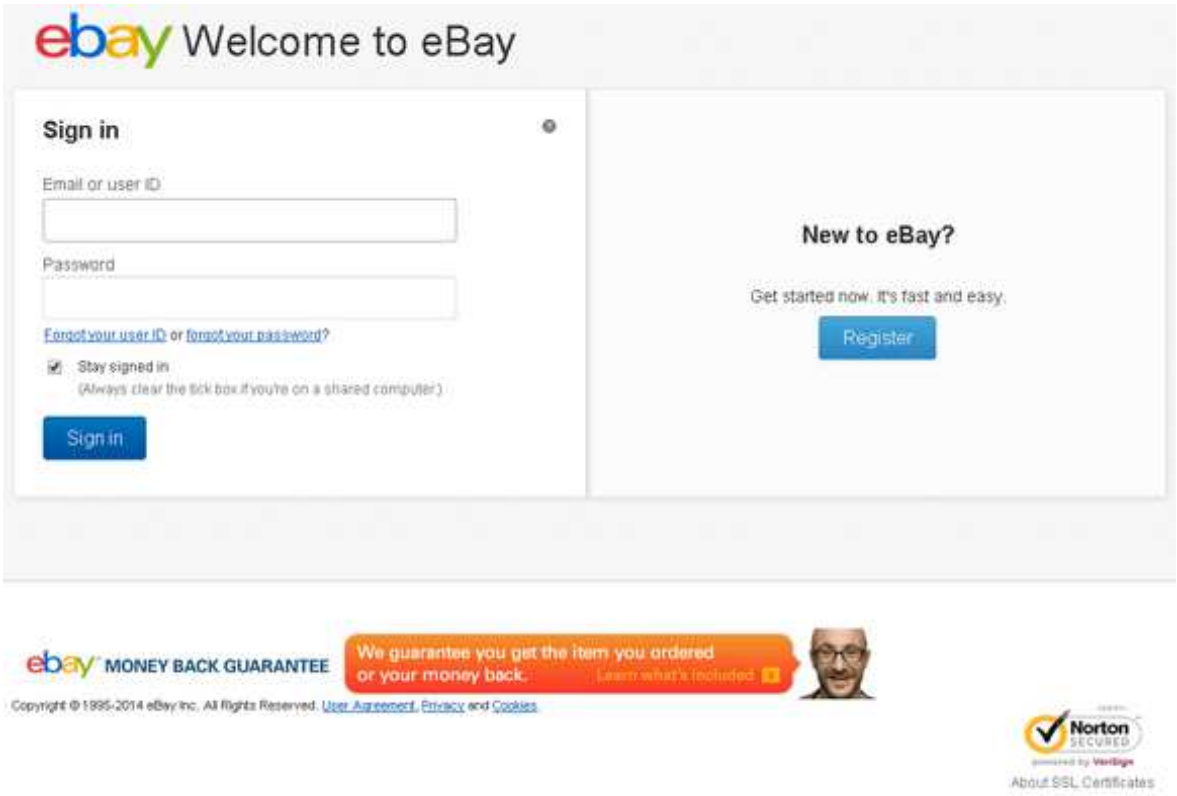


Ilustración 22- Phishing a eBay.

5. Juegos online

Excusas utilizadas para engañar al usuario: Fallos de seguridad en la plataforma del juego, problemas en la cuenta del usuario.

Objetivo: Robar cuentas, datos privados, bancarios y suplantar la identidad de los usuarios.

Ejemplos:

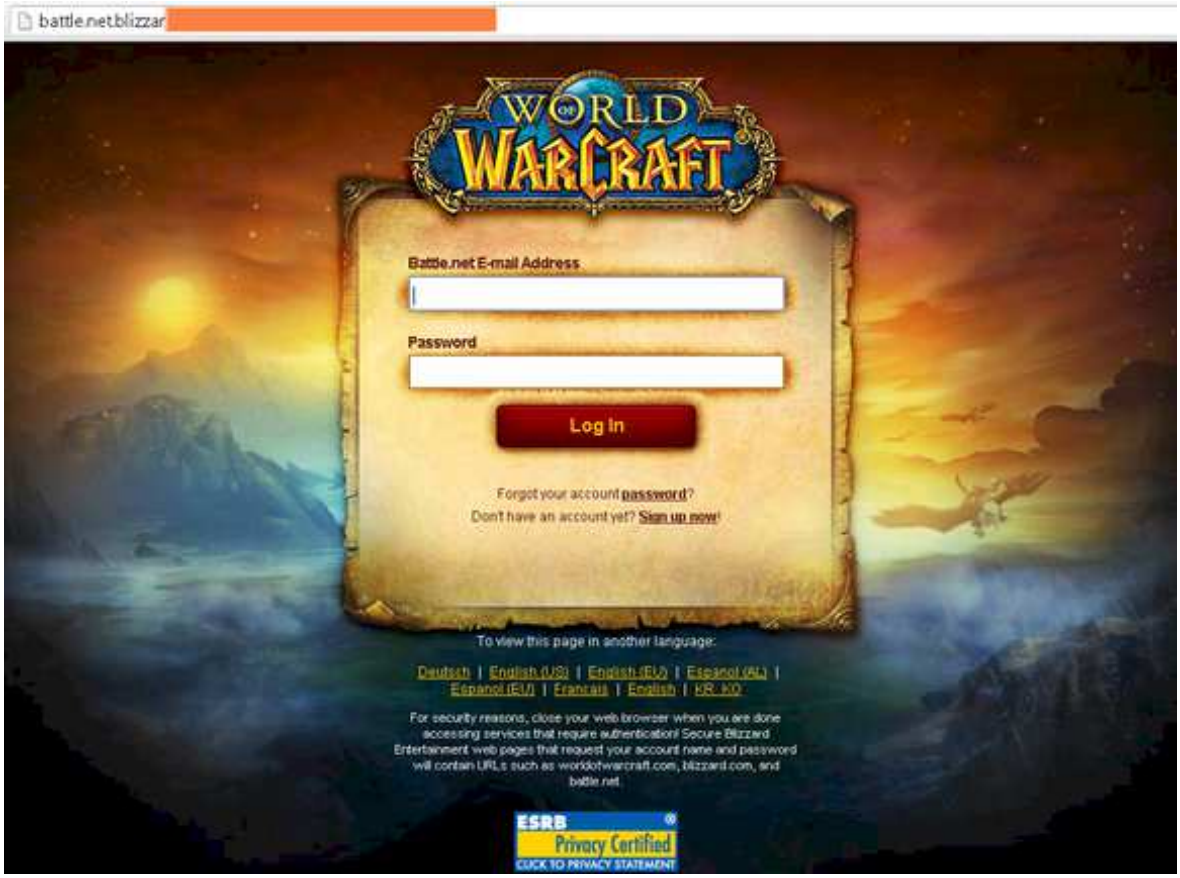


Ilustración 23- Phishing a juego.

6. Soporte técnico y de ayuda (helpdesk) de empresas y servicios (Outlook, Yahoo!, Apple, Gmail, etc.)

Excusas utilizadas para engañar al usuario: Confirmación de la cuenta de usuario, eliminación de cuentas inactivas, se detecta actividad sospechosa en la cuenta, se ha superado el límite de capacidad de la cuenta, etc.

Objetivo: Robar cuentas y datos privados de los usuarios.

Ejemplos: Phishing a Apple.

Ilustración 24- Phishing a Apple.

7. Servicios de almacenamiento en la nube (Google Drive, Dropbox, otros.)

Objetivo: Conseguir cuentas de distintos servicios de usuarios, obtener información privada.

Ejemplos: Phishing a Google Docs.

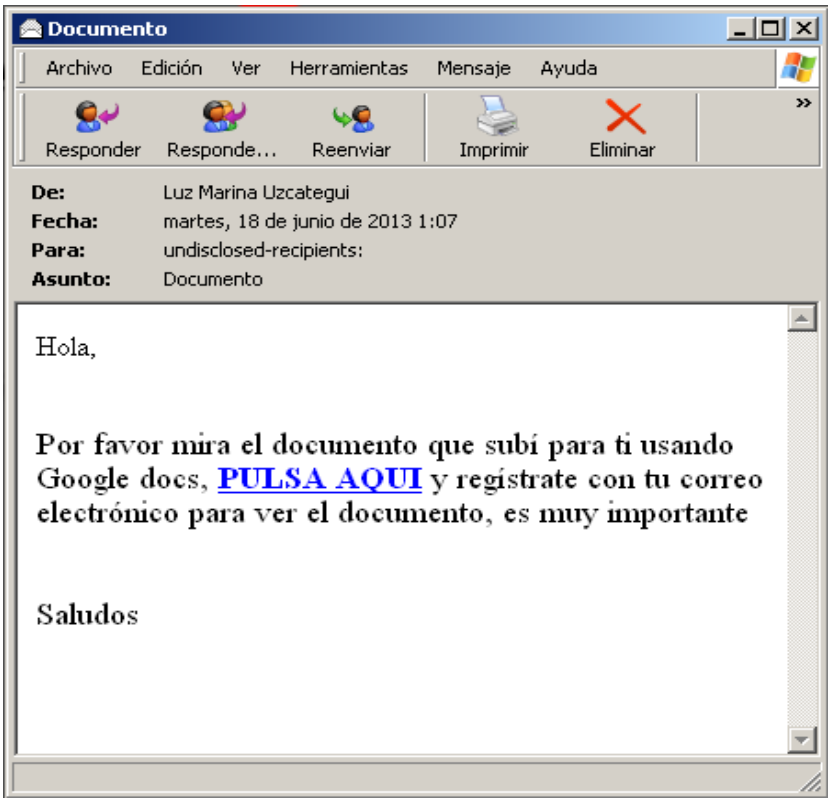


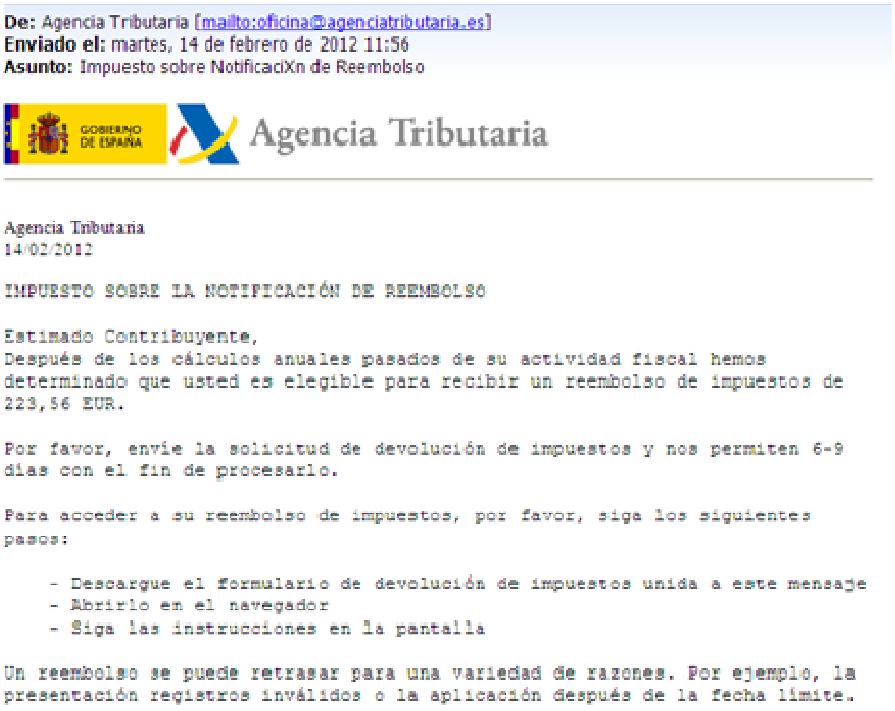
Ilustración 25- Phishing a Google Docs.

8. Phishing a servicios o empresas públicas

Excusas utilizadas para engañar al usuario: Información sobre una notificación, una multa.

Objetivo: Infectar el ordenador, robar datos privados, bancarios y estafar económicamente al usuario.

Ejemplos: Phishing a la Agencia Tributaria, a la Policía Nacional, a Correos y Telégrafos.



De: Agencia Tributaria [mailto:oficina@agenciatributaria.es]
Enviado el: martes, 14 de febrero de 2012 11:56
Asunto: Impuesto sobre NotificaciXn de Reembolso

GOBIERNO DE ESPAÑA Agencia Tributaria

Agencia Tributaria
14/02/2012

IMPUESTO SOBRE LA NOTIFICACIÓN DE REEMBOLSO

Estimado Contribuyente,
Después de los cálculos anuales pasados de su actividad fiscal hemos determinado que usted es elegible para recibir un reembolso de impuestos de 223,56 EUR.

Por favor, envíe la solicitud de devolución de impuestos y nos permiten 6-9 días con el fin de procesarlo.

Para acceder a su reembolso de impuestos, por favor, siga los siguientes pasos:

- Descargue el formulario de devolución de impuestos unida a este mensaje
- Abrirlo en el navegador
- Siga las instrucciones en la pantalla

Un reembolso se puede retrasar para una variedad de razones. Por ejemplo, la presentación registros inválidos o la aplicación después de la fecha límite.

Ilustración 26-Phishing a Agencia Tributaria.

9. Phishing a servicios de mensajería

Excusas utilizadas para engañar al usuario: El paquete enviado no ha podido ser entregado, tienes un paquete esperando, información sobre el seguimiento de un pedido, etc.

Objetivo: Infectar ordenadores, robar datos privados y bancarios de los usuarios.

Ejemplos: Phishing a DHL.

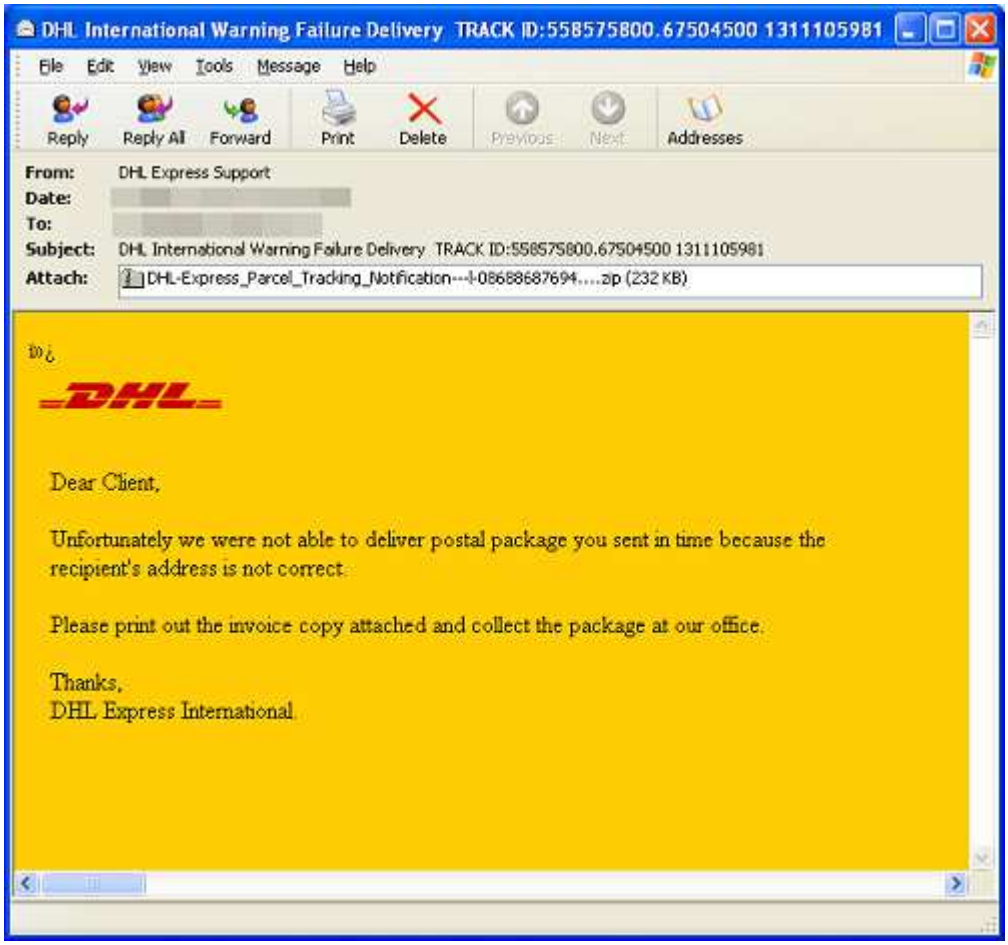


Ilustración 27- Phishing a Dhl.

10. Falsas ofertas de empleo

Excusas utilizadas para engañar al usuario: Puestos de trabajo.

Objetivo: Robar datos privados que pueden ser utilizados posteriormente con distintos fines fraudulentos.

Ejemplo: Rellena encuestas y gana mucho dinero

Escusa utilizada: Se le ofrece ganar mucho dinero al usuario por rellenar encuestas acerca de productos o marcas de empresas muy conocidas que necesitan la opinión de los consumidores con el fin de mejorar y ser más competitivas.

¿Dónde está el fraude?: el acceso a estos supuestos cuestionarios no es gratis, le cuestan al usuario al menos unos $ 250.

Ilustración 28- Falsa oferta de encuesta.

Los principales daños provocados por el phishing son:

- Robo de identidad y datos confidenciales de los usuarios. Esto puede traer pérdidas económicas para los usuarios o incluso impedirles el acceso a sus propias cuentas.
- Pérdida de productividad.
- Consumo de recursos de las redes corporativas (ancho de banda, saturación del correo, etc.).

Una de las modalidades más peligrosas del phishing es el **pharming**. Esta técnica consiste en modificar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página Web falsa.

Cuando un usuario teclea una dirección en su navegador, ésta debe ser convertida a una dirección IP numérica. Este proceso es lo que se llama resolución de nombres, y de ello se encargan los servidores DNS.

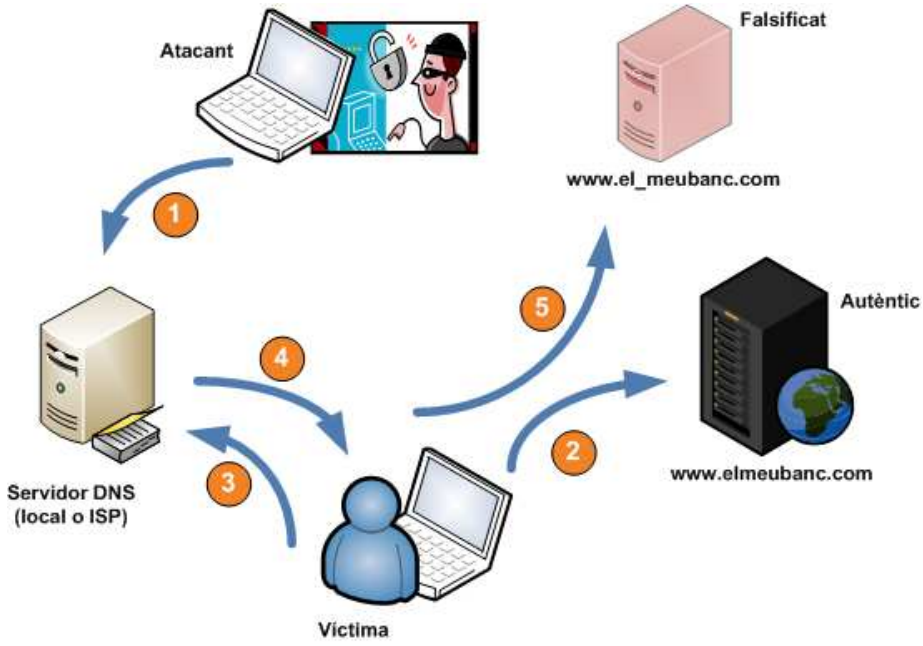


Ilustración 29- Como funciona el Pharming.

Sin embargo, existen ejemplares diseñados para modificar el sistema de resolución de nombres local, ubicado en un fichero denominado hosts.

Este fichero permite almacenar de forma local esa resolución de nombres asociadas a direcciones IP. De esta manera, aunque el usuario introduzca en el navegador el nombre de una página Web legítima, el ordenador primero consultará a ese fichero hosts si existe una dirección IP asociada a ese nombre. En caso de no encontrarla, lo consultará con el servidor DNS de su proveedor.

Esta técnica conocida como pharming es utilizada normalmente para realizar *ataques de phishing*, redirigiendo el nombre de dominio de una entidad de confianza a una página Web, *en apariencia idéntica*, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.

El canal de contacto para llevar a cabo estos delitos no se limita exclusivamente al correo electrónico, sino que también es posible realizar ataques de phishing a través de SMS, conocido como **smishing**, o de telefonía IP, conocido como **vishing.**

En el **smishing** el usuario recibe un mensaje de texto intentando convencerle de que visite un enlace fraudulento.

En el **vishing** el usuario recibe una llamada telefónica que simula proceder de una entidad bancaria solicitándole que verifique una serie de datos.

A diferencia del phishing, el pharming no se lleva a cabo en un momento concreto, ya que la modificación del fichero Hosts permanece en un ordenador, a la espera de que el usuario acceda a su servicio bancario.

¿Cómo llega?

El mecanismo empleado habitualmente es la generación de un correo electrónico falso que simule proceder de una determinada compañía, a cuyos clientes se pretende engañar. Dicho mensaje contendrá enlaces que apuntan a una o varias páginas Web que imitan en todo o en parte el aspecto y funcionalidad de la empresa, de la que se espera que el receptor mantenga una relación comercial.

Una publicación de Inteco- CERT, el 10 marzo de 2014 deja de manifiesto la utilización de phishing:

Mundial de fútbol de Brasil. Una escusa para cometer fraudes en Internet

El evento deportivo del año ya está siendo utilizado por atacantes para llevar a cabo acciones maliciosas por la Red. Debemos mantenernos informados para evitar caer en sus redes.

Ya estamos en la cuenta regresiva del Mundial de Fútbol: Brasil 2014. Como no podía ser de otra forma, los aficionados al fútbol ya están con los preparativos: comprando camisetas de su selección, reservando billetes de avión y alojamientos en Brasil y por supuesto, gestionando las entradas para ver los partidos en vivo.

Sin embargo, los futboleros no son los únicos que ya se están movilizando, como era de esperar, y como ya han hecho en otros acontecimientos importantes (muertes de personas conocidas, catástrofes naturales, trágicos accidentes, etc.), los atacantes están poniendo en marcha campañas fraudulentas por Internet que utilizan como escusa el evento deportivo del año para engañar a los usuarios.

¿Cuáles son los principales reclamos con los que intentarán engañar?

1. Mensajes que aseguran que hemos sido ganadores de una entrada (o cualquier otro premio)

Hemos tenido la suerte, que sin hacer nada, hemos sido obsequiados con una entrada para un partido del Mundial. Sólo tenemos que acceder a un link para imprimir el ticket. Lo que no explica el mensaje, es que esa URL nos puede redirigir a una Web fraudulenta capaz de descargar virus en nuestro ordenador o suplantar la identidad de una empresa o servicio para que introduzcamos nuestros datos privados, los bancarios. Para captar nuestra atención, algunos mensajes utilizan nombres de jugadores de fútbol conocidos internacionalmente, como Neymar, Messi y Cristiano o de la mascota oficial del mundial, Fuleco.

Ilustración 30- Ejemplo de correo fraudulento.

Spear Phishing

El "*spear phishing*" es una variante del *Phishing*. Se traduce como "pesca de arpón" porque es un ataque de *Phishing* dirigido a un objetivo específico.

Los timadores de "*spear phishing*" envían mensajes de correo electrónico que parecen auténticos a todos los empleados o miembros de una determinada empresa, organismo, organización o grupo.

Podría parecer que el mensaje procede de un jefe o de un compañero que se dirige por correo electrónico a todo el personal (por ejemplo, el encargado de administrar los sistemas informáticos) y quizá incluya peticiones de nombres de usuario o contraseñas.

En realidad, lo que ocurre es que la información del remitente del correo electrónico ha sido falsificada. Mientras que las estafas de suplantación de identidad (*phishing*) tradicionales están diseñadas para robar datos de personas, el objetivo de las de *spear phishing* consiste en obtener acceso al sistema informático de una empresa.

Si responde con un nombre de usuario o una contraseña, o si hace clic en vínculos o abre datos adjuntos de un mensaje de correo electrónico, una ventana emergente o un sitio Web desarrollado para una estafa de "*spear phishing*", puede convertirse en víctima de un robo de datos de identidad y poner en peligro a su organización.

Las estafas de "*spear phishing*" también se dirigen a personas que utilizan un determinado producto o sitio Web. Los timadores utilizan toda la información de que disponen para personalizar al máximo posible la estafa de suplantación de identidad (phishing).

Recolección de hábitos de las víctimas potenciales

Este método se basa en la creación de perfiles ficticios e infiltrarse en redes sociales o en servicios de mensajería, de esta forma se puede recolectar información acerca de los hábitos de las víctimas potenciales. Para las redes sociales solo basta con echar un vistazo en fotos de viajes o la información personal que se proporciona, de la misma forma si se puede tener comunicación basta con que se entable una relación para poder obtener la información que se necesita. Un adolescente que no reciba la atención requerida por parte de sus padres puede conseguir un "amigo incondicional" en línea, a quien le cuente todo lo que le pasa y todo lo que hace.

Son incontables los casos de secuestros y robos que se han hecho, al levantar la información necesaria obtenida de manera fácil gracias a la ingenuidad y falta de malicia de las víctimas.

Una publicación en el diario *La Voz del Interior*, el 24 de septiembre de 2013, deja en evidencia este tipo de engaños.

"Ordenan a Facebook notificar a contactos de un perfil falso".

"Río Cuarto. El juez federal de Río Cuarto, Carlos Ochoa, hizo lugar a una demanda presentada por el abogado local Enrique Novo, para reclamar a Facebook por un perfil falso con su nombre. El magistrado no sólo ordenó cerrar la cuenta apócrifa, sino que –en un fallo que sería inédito para el país– ordenó a Facebook informar en 48 horas a todos los contactos que tenía esa cuenta "trucha" el motivo por el cual fue cerrada.

Novo, docente en la Universidad Nacional de Río Cuarto y exconcejal, contó que tiene un perfil en la red social con su apodo "Quique Novo", pero meses atrás advirtió que existía otro con su nombre completo: "Enrique Novo", que decía ser "egresado de la Universidad Nacional de Río Cuarto", con lo que se prestaba a la confusión.

Aseguró que primero hizo el reclamo por la vía extrajudicial, pero le respondieron que la biografía reportada no infringía "la norma comunitaria de Facebook sobre identidad y privacidad". Como el autor de la cuenta "trucha" seguía produciendo comentarios, Novo envió una carta documento y se presentó ante la Justicia.

No hace falta ser famoso ni poderoso para verse afectado y angustiado. Cualquier persona que ve que un tercero se hace pasar por él sentirá angustia e incertidumbre. Todos tenemos la facultad de solicitar que se protejan esos derechos", explicó a este diario. El reclamo judicial fue por una medida autosatisfactiva, es decir, para que cese la anomalía. Novo no planteó ninguna acción penal ni resarcitoria."

Dumpster diving o Trashing (buceo de basurero)

Se refiere al acto de husmear entre la basura, de esta manera se pueden obtener documentos con información personal o financiera de una persona.

Revisar los desperdicios y la basura ("trashing" en inglés), es otro método popular que aplica la Ingeniería Social.

Ilustración 31- Trashing

Pretexting

El pretexting (pretextos) implica llamar por teléfono al usuario y pedirle cierta información, generalmente simulando ser alguien que precisa su ayuda. Esta técnica puede funcionar bien si se usa mediante aquellos usuarios de bajo nivel técnico y que tengan acceso a información sensible.

La mejor estrategia para empezar es con nombres reales y pequeñas peticiones al personal de la organización que esté esperando algo. En la conversación, el atacante simula necesitar ayuda de la victima (Mucha gente está

dispuesta a hacer pequeñas tareas que no sean percibidas como algo sospechoso). Una vez establecido el contacto, el atacante puede pedir algo más sustancial.

3.3. Conceptos de Redes Sociales

Las redes sociales son “comunidades virtuales”.

Es decir, plataformas de Internet que agrupan a personas que se relacionan entre sí y comparten información e intereses comunes. Este es justamente su principal objetivo: entablar contactos con gente, ya sea para re encontrarse con antiguos vínculos o para generar nuevas amistades.

En las redes sociales los usuarios interactúan con personas de todo el mundo con quienes encuentran gustos o intereses en común. Funcionan como una plataforma de comunicaciones que permite conectar gente que se conoce o que desea conocerse, y que les permite centralizar recursos, como fotos y videos, en un lugar fácil de acceder y administrado por los usuarios mismos.

En la actualidad estas son una de las principales herramientas de comunicación utilizadas por los adolescentes. El número de usuarios que tiene cada una, ha aumentado de una manera muy rápida gracias a las diversas utilidades que se les pueden dar: desde compartir información, fotos y pensamientos con gente en el aspecto personal, hasta promocionar productos u ofrecer servicio al cliente en lo empresarial.

3.3.1. Orígenes de las redes sociales

El primer antecedente se remonta a 1995, cuando un ex estudiante universitario de los Estados Unidos creó una red social en Internet, a la que llamó

classmates.com (compañeros de clase.com), justamente para mantener el contacto con sus antiguos compañeros de estudio.

Pero recién dos años más tarde, en 1997, cuando aparece SixDegrees.com (seis grados.com) se genera en realidad el primer sitio de redes sociales, tal y como lo conocemos hoy, que permite crear perfiles de usuarios y listas de "amigos".

A comienzos del año 2000, especialmente entre el 2001 y el 2002, aparecen los primeros sitios Web que promueven el armado de redes basados en círculos de amigos en línea. Este era precisamente el nombre que se utilizaba para describir a las relaciones sociales en las comunidades virtuales. Estos círculos se popularizaron en el 2003, con la llegada de redes sociales específicas, que se ofrecían ya no sólo para re encontrarse con amigos o crear nuevas amistades, sino como espacios de intereses afines.

Las claves para el éxito de las redes sociales se fundamentan en tres variables conocidas como ***"Las 3 Cs".***

Comunicación (porque estimulan el diálogo).
Comunidad (porque permiten integrar grupos afines).
Cooperación (porque promueven acciones compartidas).

En la actualidad existen más de 200 redes sociales, con más de 800 millones de usuarios en todo el mundo. Una tendencia que crece cada mes.

3.3.2. Evolución de las redes sociales

Las redes sociales siempre han existido. El ser humano es social por su naturaleza y por lo tanto los que cambian y evolucionan son los canales de comunicación, adaptándose en todo momento al entorno que les rodea. Creen que la más simple fogata y señales de humo, pasando por los trueques, los mercados. Todo esto, fue el desencadenante de Internet la "Gran Revolución", y que a partir de este se desencadenó el mundo tecnológico que hoy conocemos.

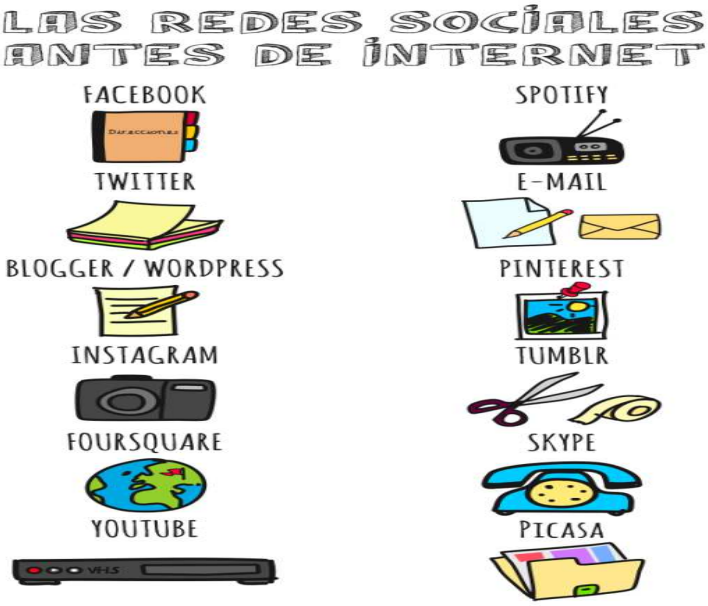


Ilustración 32- Las redes sociales antes de Internet

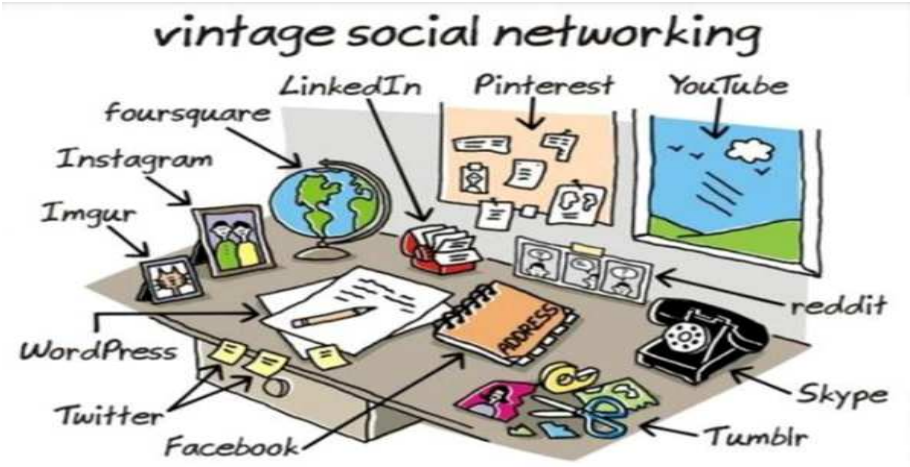


Ilustración 33 – Evolución de las redes sociales

Redes Sociales más conocidas

Según un estudio realizado por Leverage, publicado por Mediabistro, el 21 de enero de 2014.

- **Facebook:** Reporta mil millones de usuarios activos. Cada día la comunidad comparte en total 2,5 mil millones de piezas de contenidos.
- **Google+:** Tiene 400 millones de usuarios activos, y un crecimiento de 925 mil nuevos usuarios cada día.
- **Twitter:** 560 millones de usuarios activos. En esta red 5,700 Tuits se publican cada segundo.
- **LinkedIn:** Mantiene 240 millones de usuarios activos, y el 79% de ellos tiene más de 35 años.
- **Pinterest:** tiene 70 millones de usuarios activos (32% es varón y el 68% es conformado por mujeres).
- **Instagram:** Cuenta con una comunidad de 150 millones de personas activas. La marca más seguida es MTV.

De acuerdo al tráfico y popularidad de cada una, basados en el índice que poseen en Alexa, sitio Web dedicado a monitorear el tráfico de los sitios de Internet. Las redes sociales más conocidas son Facebook, Google +, Twitter, Linkedln, Pinterest e Istragram.

Facebook

Facebook es la red social más exitosa, conocida y popular de Internet. Es una herramienta social para conectar personas, descubrir y crear nuevas amistades, subir fotos y compartir vínculos se paginas externas y videos.

¿Por qué el enorme éxito de Facebook?

- La facilidad de compartir contenido, ya sea links, fotos o videos.
- La posibilidad casi sin límites de subir las fotos.
- La interface sencilla, aun para el usuario no experimentado en la navegación Web.
- La facilidad de convertirse en miembro y crear una cuenta.
- La facilidad que agrega el chat.
- La integración de mensajes y correos electrónicos.
- Las recomendaciones de nuevos amigos, muchas veces acertadas.
- Las exitosas páginas de fans beneficiosas para negocios, empresas y marcas.
- La posibilidad de los desarrolladores de crear aplicaciones para integrarlas y ganar dinero por ello.

Google+

Es la más nueva y reciente de las redes sociales y ya cuenta con una inmensidad de miembros. Gracias al inmenso protagonismo y poder de Google en Internet, puede llegar a ser una de las redes más grandes y poderosas. Brinda facilidades para crear redes de amigos y organizarlos en los llamados *círculos*.

Posibilita subir contenido para compartir de forma sencilla. Se integra con otros servicios populares de Google como Gmail, GMaps, Calendario, Docs, etc.

Twitter

Twitter es una red social de microblogging, o sea una red para publicar, compartir, intercambiar, información, mediante breves comentarios en formato de texto, con un máximo de 140 caracteres, llamados Tweets, que se muestran en la página principal del usuario.
Es la plataforma de comunicación en tiempo real, más importante que existe en la actualidad.
Los usuarios pueden suscribirse a los Tweets de otros, a esto se le llama "seguir" y a los suscriptores se les llaman "seguidores".
Posee un especial atractivo para actualizar el estado rápidamente desde dispositivos portables como los teléfonos celulares y para compartir noticias en tiempo real.
La principal característica de Twitter es su sencillez, la facilidad y diversidad de formas existentes para conectarse a dicha red y poder comunicarse con otros.

LinkedIn

LinkedIn es una red orientada a los negocios y para compartir en el ámbito profesional. Están representadas en ella la gran mayoría de las empresas de más de 200 países. Indispensable para la promoción profesional y muy útil para buscar y compartir información técnica y científica.

Pinterest

Se ha convertido en la tercera red social más visitada en los Estados Unidos, detrás de Facebook y Twitter.
Fue seleccionada como uno de los 50 mejores sitios del 2011.
Es un sitio donde compartir, encontrar y organizar colecciones de imágenes o videos. Funciona como una especie de un enorme tablón digital, donde vamos pegando imágenes y vídeos (esto se conoce como Pin), que por algún motivo nos interesan ya sea que los hayamos subido de nuestro equipo o encontrados en una página de Internet.

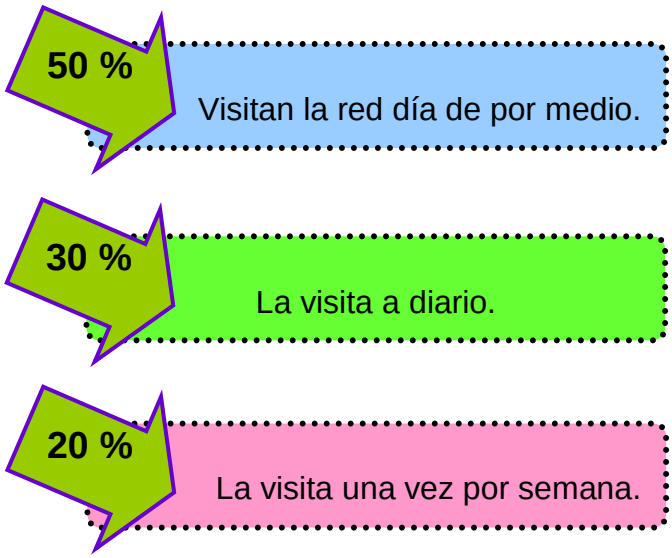
Instagram

Es una aplicación muy popular para dispositivos móviles, permite editar, retocar y agregarle efectos a las fotos tomadas con los celulares, facilita compartirlas en las redes sociales y desde el momento que es posible navegar y explorar las fotos de otros usuarios registrados, se considera una red social. La usan más de 150 millones de usuarios.

3.3.3. Los adolescentes y las redes sociales

La mayoría de quienes están en alguna red social son jóvenes.

El 80 % de los usuarios de redes sociales en todo el mundo, tiene entre 12 y 30 años. Y la frecuencia de uso entre los adolescentes de 12 a 18 años es muy alta.



¿Por qué son tan populares entre los adolescentes?

Cada día más adolescentes eligen unirse a una red social. Su crecimiento en los últimos años llegó de la mano de la llamada Web 2.0, que propuso un nuevo uso de Internet.

Los adolescentes –según explican ellos mismos- están en las redes sociales por dos motivos:

¿Qué es lo que más valoran los adolescentes de sí mismos? *La popularidad.* ¿Y qué necesita un adolescente para ser popular? Amigos, humor y espontaneidad. Así lo reflejó la encuesta realizada en el Colegio San José, entre 160 alumnos de nivel medio. Ser popular es tener muchos amigos. La identidad de los adolescentes no puede entenderse sin sus amigos. Y sin ellos, tampoco es fácil comprender los usos que hacen de los medios y las tecnologías. Los chicos de hoy, aun rodeados de pantallas valoran a los amigos tanto como los de ayer. Solo que Internet generó nuevas maneras de relacionarse, nuevas formas de sociabilidad.

Las pantallas son tema de conversación entre ellos. Son además soportes de su vida social. Para comunicarse, esta generación puede hablar

por teléfono de línea o celular, enviar un mensaje de texto, mandar un email, chatear, bloggear, encontrarse en una red social.

Inmersos en este mundo tecnológico, es comprensible que la vida social de los adolescentes pase por las pantallas. Los chicos quieren aumentar su lista de "amigos". Y para conquistar la amistad del otro, a veces comparten información personal. El concepto de "amistad" virtual y real, no es el mismo. Y ellos lo saben. Pero los amigos de la Red son también "amigos". Y suman. Para el adolescente, *el anonimato y la intimidad ceden ante el deseo de fama y popularidad.*

¿No son conscientes los chicos de que esta exposición trae riesgos? Cuando un adolescente construye su blog o su perfil en una red social, suele pensar que sólo lo ven sus amigos, o quienes están interesados en lo que dice. No piensan que cualquiera que navegue en la Red, conocido o no, puede ver lo que escribió. Los chicos no creen en los riesgos de Internet porque se sienten "autoinmunes" o porque piensan solo en sus amigos.

¿Cómo funciona una red social?

Para crear y mantener una página personal en una red social, hay que seguir diferentes pasos:

1. Crear un perfil de usuario. Este perfil consiste en las características que la persona quiere dar a conocer sobre sí misma, para incorporarse como nuevo miembro en una red social. En el perfil, la gente incluye los datos personales que quiere: nombre, dirección electrónica, actividades, gustos, intereses, etc. De cualquier modo, sólo con el nombre y dirección de email ya puede ser integrante.

2. Incorporar a los primeros amigos. Una vez creada la página, su autor "invita" a sus amigos vía email a formar parte de su red. Cuando estos aceptan la invitación y ya forman parte de la red, pueden sugerir la incorporación de otros conocidos.

3

Intercambiar mensajes, subir fotos, compartir música. Una vez que el usuario tiene un grupo social en la red, puede comunicarse con sus integrantes, intercambiar información, subir fotos, compartir música, ver el Perfil de otro, etc.

4

Hacer crecer la lista de amigos. Como el objetivo de una red social es agrupar personas y lograr más “amigos”, los usuarios siguen invitando a más gente a participar en su red (amigos de amigos) y de esta manera, lograr que la lista se agrande con Un estudio amigos de amigos de amigos de amigos.

En la encuesta realizada a los alumnos del Colegio San José, dio como resultado que el 98 % de los alumnos pertenece a alguna red social. Según los adolescentes, manifiestan estar en la red social porque:

Para tener mí sitio personal.

- Porque es como un juego y me divierte.
- Porque cuento quién soy y, a veces, quién me gustaría ser.
- Porque subo fotos, videos y música para compartir con otros.
- Porque dejo comentarios en el sitio de otras personas.

Para construir una red de amigos.

Y reencontrarme con gente que hace mucho tiempo no veo.

- Para estar al día con mis amigos de la vida real.
- Para chatear y enviar mails a través de la red.

- Para estar en grupo y conocer gente nueva.
- Para enterarme de eventos y novedades.
- Para agrandar mi grupo de “amigos” con amigos de amigos.
- Para organizar reuniones.

Los riesgos en Internet y las redes sociales para los adolescentes

El riesgo mayor con Internet, es que los adolescentes no siempre son conscientes de lo que puede ocasionar un uso no responsable de la Web. La confianza que tienen en ellos mismos es superior a la posibilidad de pensar en situaciones difíciles que puede generar la Red. Esto hace que las prevenciones y recaudos que los chicos toman respecto de Internet, sean menores.

De hecho, en la encuesta realizada al colegio San José, arrojó como resultado que de 160 alumnos, el 100 % de los adolescentes de 12 a 18 años utiliza Internet.

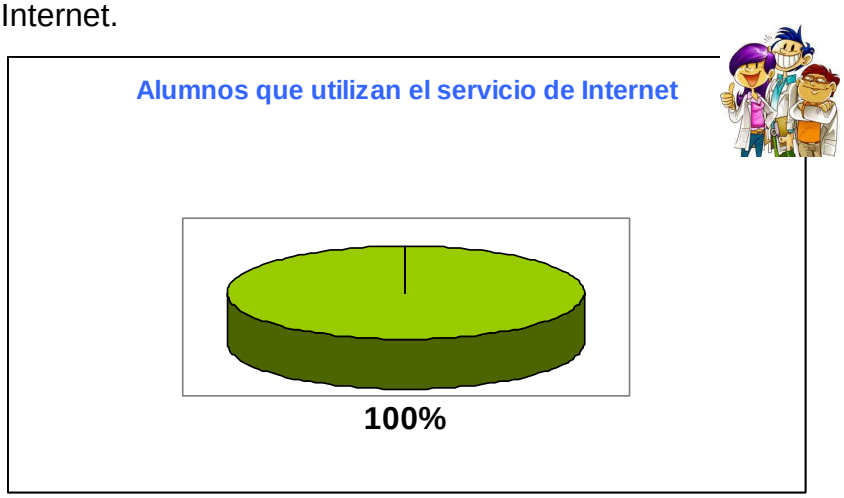


Ilustración 34 – Porcentaje de alumnos que utilizan Internet.

De los adolescentes encuestados el:

95 %	No cree en los riesgos de Internet.
90 %	Se siente inmune frente a lo que puedan encontrar.
75 %	Cree en todo lo que dice la Red.
60 %	Cree que sólo amigos ven su página personal.
90 %	Dice que en su casa no hay reglas de uso.

Los adolescentes, como se ve, no suelen ser conscientes de los riesgos que puede traer un uso no responsable de las redes sociales. Y aun, quienes tienen información sobre estos riesgos, no siempre trasladan lo que saben, a la acción. En general se sienten seguros de lo que hacen en Internet.

Los adolescentes en su propia palabra dicen:

> "Me tengo confianza, soy hábil con la tecnología".
> "Es más importante conocer gente, que pensar en los riesgos".
> "Me gusta abrir mi página para que la vean todos".
> "No me imagino qué riesgos pueda tener estar en una red social".
> "La red social es la responsable de los riesgos y los tiene controlados".

Los adolescentes son vulnerables y en muchos casos no están en condiciones para manejar los riesgos latentes en las redes sociales a la hora de intimar o contactarse con desconocidos sumado a que muchas veces mienten a la hora de anotar su edad para lograr el acceso a las mismas.

Compartir información personal y encontrarse con desconocidos en la vida real, son los mayores riesgos del uso de las Redes Sociales.

Si los adolescentes usan Internet o redes sociales desde equipos comunitarios, como una computadora de escritorio o una portátil tipo notebook, cualquier padre puede conocer qué páginas visitó su hijo o cuál fue su actividad en la red con sólo revisar el historial, amén de poder instalar programas que impiden el acceso a determinadas páginas o rubros. Sin embargo, con el auge de los teléfonos celulares conectados la situación cambia, no sirve revisar el historial de visitas o la actividad en las redes sociales, por lo que es esencial el acompañamiento y la educación.

Por eso lo más importante es educar, explicar, para que sean autónomos, se puedan defender.

Como las redes sociales se organizan en torno a las páginas Web de los usuarios, los riesgos más frecuentes en este caso, tienen que ver con la construcción y el contenido de los sitios personales.

Algunos riesgos:

- Abrir los sitios para que cualquiera los pueda ver.
- Dar información personal.
- Subir fotografías, propias o ajenas, que reflejen situaciones de intimidad.
- Hacerse “amigos” de gente que no conocen.
- Encontrarse en persona con “amigos” que sólo conocieron en la Red.

En Estados Unidos, una investigación del año 2008 reflejó que el 30 % de los adolescentes que usan Internet se comunican “on line” con personas que no conocen. Y un 10 % de ellas ha establecido vínculos más estrechos.

Un estudio entre países de la Unión Europea determinó que el 50 % de los adolescentes suele dar información personal en Internet y casi un 10 % se encuentra personalmente con gente que conoció en la Web.

La información que damos acerca de nuestra vida diaria en las redes sociales es mucha, y cada vez más. Quizás en muchos casos sea demasiada. Pero más allá de la pérdida de privacidad que muchos usuarios de estas plataformas asumen en pro de las ventajas que conllevan, *el uso de las redes sociales o, mejor dicho, contar demasiadas cosas de nosotros mismos en estos sistemas conlleva riesgos de seguridad importantes*. La ingeniería social, el robo de identidades, el ciberacoso son solo algunas de las amenazas que proliferan al calor de estas plataformas. Saber qué debemos contar y cómo es clave para nuestra seguridad.”

Los sextorsionadores utilizan las redes sociales para incrementar su amenaza sobre las víctimas.

Resultado arrojado de la encuesta a los alumnos de la Institución, sobre la percepción de los adolescentes en cuanto a la seguridad de sus datos en las redes sociales.

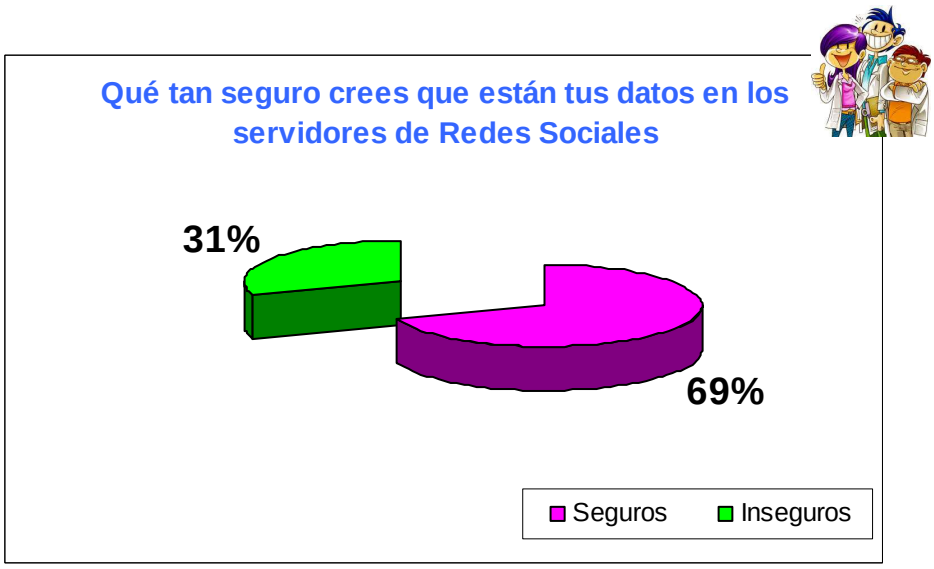


Ilustración 35- Porcentaje de percepción de seguridad de los datos en las redes sociales.

¿Qué se puede hacer frente a este panorama?

Es importante tener conocimiento de este tipo de prácticas ya que la información es vital para todos, por este motivo es necesario que los adolescentes tomen una serie de precauciones para evitar este tipo de ataques. Ya que la desinformación es la principal herramienta que usan los Ingenieros Sociales para sus prácticas. Es por ello que se visualiza la necesidad de incorporar la página Web sobre este tema, para que sea utilizada por los alumnos y docentes de la Institución Educativa. Educando a los adolescentes, para que sean concientes y responsables.

4. Modelo Teórico

Para conocer la realidad con la que nos enfrentábamos, utilizamos una encuesta (ver Anexo A y Anexo B) como método de estudio, ya que era la forma más sencilla de poder llegar a los alumnos y docentes de la Institución.

Además se habló con los alumnos y docentes, sondeando a grandes rasgos si eran conscientes de los riesgos que puede traer un uso no responsable de las redes sociales e Internet.

La Institución Educativa que se tomo como referencia para llevar a cabo las encuestas es el colegio San José, de la localidad de San Agustín.

La población a la que se le realizó la encuesta fue a los alumnos de nivel medio con edades comprendidas entre los 12 y 18 años en su mayoría; conformando un total de 160 alumnos encuestados. Y a los docentes, conformando un total de 25 docentes encuestados.

Así esta investigación se buscó el grado de sensibilización de los alumnos y docentes sobre el grado de conocimiento que tenían sobre la Ingeniería Social y el tratamiento de sus datos en las nuevas tecnologías y el uso de las redes sociales.

Las encuestas fueron elaboradas utilizando la herramienta Google Drive. Posteriormente se cargaron las respuestas de los alumnos y docentes, procesando los datos con dicha herramienta. Con el que se obtuvieron los porcentajes de las encuestas para poder comparar los resultados obtenidos.

A lo largo de este proyecto hemos incluido gráficos estadísticos y análisis de los datos, de las encuestas realizadas a la Institución.

De un total de 160 alumnos encuestados, el 66% (105 alumnas) pertenece al género femenino y el 34 % (55 varones) al género masculino.

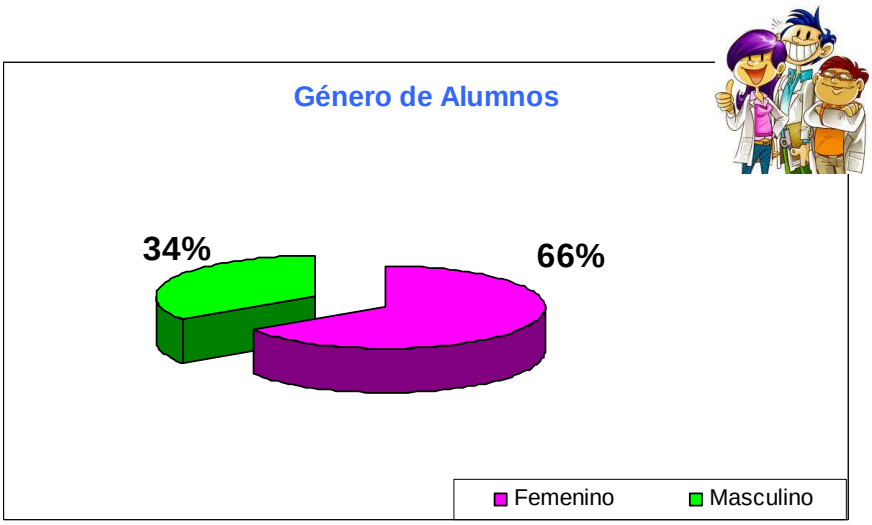


Ilustración 36- Porcentaje de alumnos, por género.

De la encuesta realizada, el 76 % de los alumnos han recibido correos electrónicos que promocionaban servicios no solicitados. De este porcentaje el 53 % de los alumnos visitó dichas páginas Web (Ver Ilustración 4 y 5). A tener en cuenta:

4.1. Privacidad- Correo Electrónico

Cada día, el buzón de nuestro correo electrónico se satura por mensajes colectivos de todo tipo: Consejos para meditar, traer el amor y la suerte a tu vida, chistes, o noticias alarmantes que debes enviar a todos tus conocidos; y si siguiéramos; la lista es larguísima. El 76 % de los mails que se envían, no fueron solicitados.

Lo que muchos no saben es que estos mails son diseñados por personas malintencionadas, ingenieros sociales, que buscan obtener listas de correos a partir de los mensajes reenviados que posteriormente podrán utilizar para enviar publicidad o cualquier tipo de programa que ocasione un daño al equipo o a la información.

Es por ello que a continuación te compartimos algunos consejos para hacer un uso seguro de tu correo electrónico:

- No abras correos de remitentes desconocidos, si lo haces y trae un archivo adjunto, bórralo sin abrirlo.

- Cuando reenvíes un correo a un grupo de personas, procura escribir las direcciones en el campo "CCO" (con copia oculta), así la lista de tus contactos no será visible para quien lo reciba y los estarás protegiendo.
- Antes de reenviar un mail, borra del cuerpo de texto las direcciones de aquellos que lo enviaron anteriormente.
- Cuando registres tu cuenta en algún formulario de Internet procura desactivar la casilla de aceptación para el envío publicidad o indica que no deseas recibir información del sitio y proveedores si fuera el caso.
- Publica tu correo electrónico en Internet sólo cuando sea necesario. Cuando publicas tu correo electrónico para que te escriban en un foro, blog, aparece a la vista de todo el mundo. Hay programas que rastrean páginas Web y recopilan los correos electrónicos de los perfiles.
- Al usar tu correo electrónico desde sitios públicos, cierra todos los programas utilizados, las sesiones iniciadas y el explorador. Es recomendable eliminar archivos temporales y cookies al terminar tu navegación. .
- Siempre que descargues archivos adjuntos solicita al antivirus que lo analice antes de abrirlo, en especial si desconoces el destinatario.
- Las entidades bancarias y financieras, así como empresas de correo electrónico o redes sociales nunca solicitan tus datos a través de correo electrónico. Si recibes alguno, comunícate con tu administrador o directamente con la compañía y solicita asesoría.
- Ninguna compañía seria dona o paga dinero por reenviar un correo electrónico.

Recuerda, que tu seguridad de pende de ti, de tu atención en el uso de Internet, de aplicar los consejos básicos y de enseñárselos a tu familia y amigos.

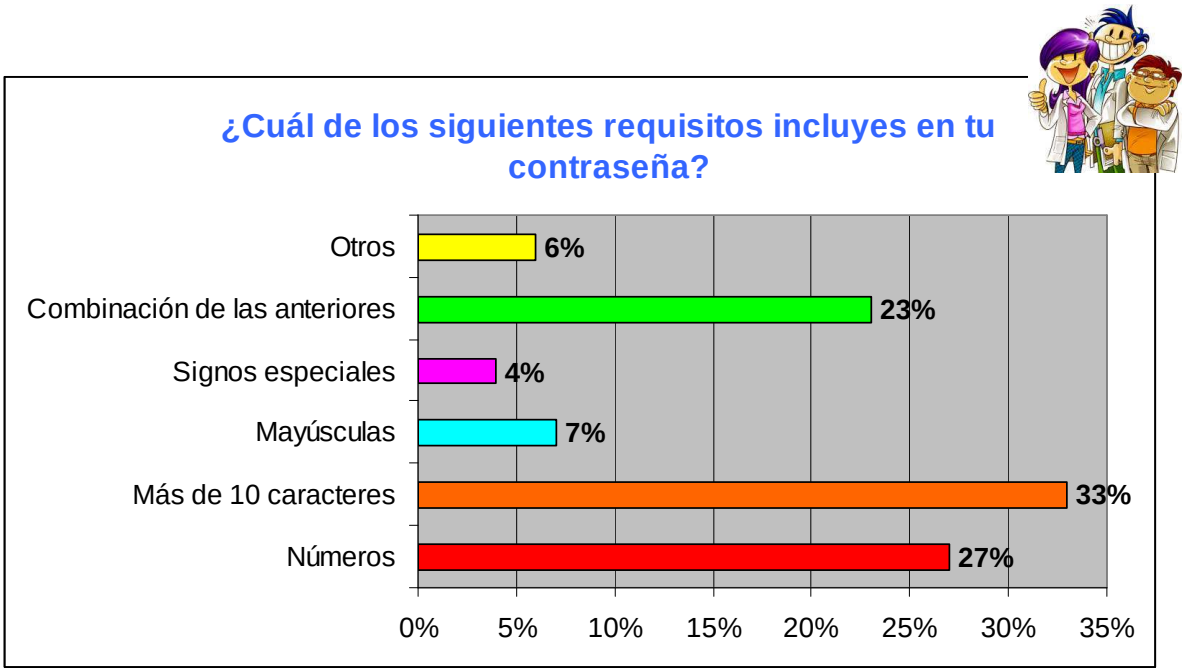


Ilustración 37- Porcentaje de requisitos para crear la contraseña que tienen en cuenta los alumnos.

En los requisitos que tienen en cuenta los alumnos para crear su contraseña visualizamos que el 33 % utiliza más de 10 caracteres, el 27 % utiliza números, el 23 % utiliza combinación de signos, mayúsculas, caracteres y números.

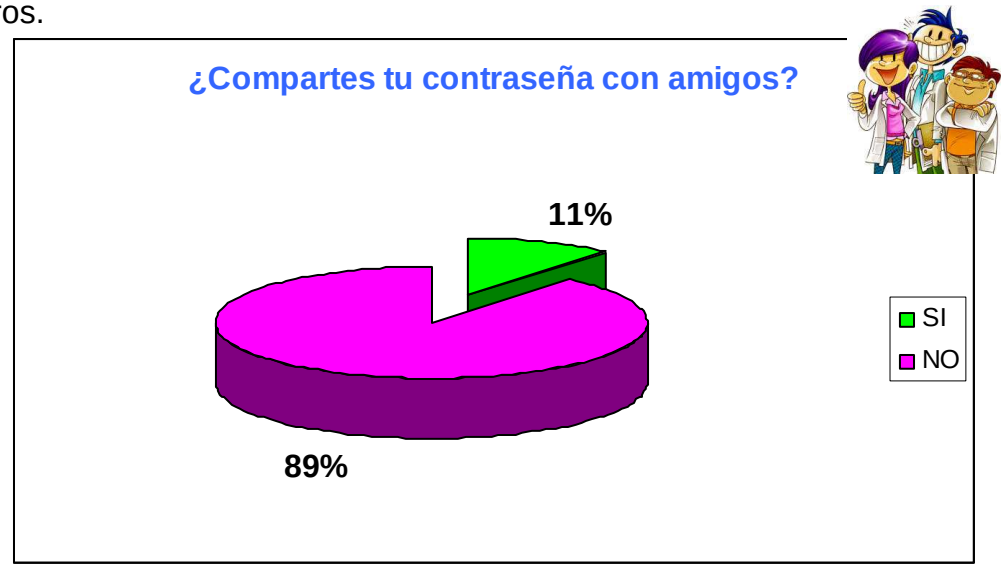


Ilustración 38- Porcentaje de alumnos que comparten su contraseña

En cuanto a la cantidad de alumnos que comparten su contraseña, podemos apreciar que es un porcentaje muy bajo, sólo el 11 %. Esto nos pone de manifiesto que los alumnos en este punto tienen conocimiento.

4.2. Selección de contraseñas

Muchas contraseñas de acceso son obtenidas fácilmente porque involucran el nombre u otro dato familiar del usuario y, además, esta nunca (o rara vez) se cambia.

Normas de Elección de Claves

Se debe tener en cuenta los siguientes consejos para crear una contraseña:

- No utilices contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).
- No uses contraseñas completamente numéricas con algún significado (teléfono, D.N.I., fecha de nacimiento, patente del automóvil, PIN).
- No utilices terminología técnica conocida que otra persona podría conocer.
- Elige una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.
- Deben ser largas, de 8 caracteres o más.
- Tener contraseñas diferentes en máquinas diferentes y sistemas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas. Esto permite que si te roban una contraseña, no te roben los accesos a todos los lugares a los cuales ingresas.
- Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son:
  - ✓ Combinar palabras cortas con algún número o carácter de

puntuación: soy2_yo3.

- ✓ Usar un acrónimo de alguna frase fácil de recordar: A río Revuelto Ganancia de Pescadores: ArRGdP.
- ✓ Añadir un número al acrónimo para mayor seguridad: A9r7R5G3d1P.
- ✓ Mejor incluso si la frase no es conocida: Hasta Ahora no he Olvidado mi Contraseña: aHoeIIo
- ✓ Elegir una palabra sin sentido, aunque pronunciable: taChunda72, AtajulH, Wen2Mar
- ✓ Realizar reemplazos de letras por signos o números.

Luego que selecciones tu contraseña, debes considerar no entregar por ningún motivo la misma a ninguna persona, ya que si lo haces esa persona podría robar tu información (nombre, usuario, fotos, blog, chat) e incluso hacerse pasar por ti ante otras personas.

De la encuesta, se obtuvo que el 98 % de los alumnos pertenecen a alguna red social. Mientras que el 2 % no utiliza este servicio. Como se puede observar, es alto el porcentaje de usuarios de redes sociales. (Ver Ilustración 6).

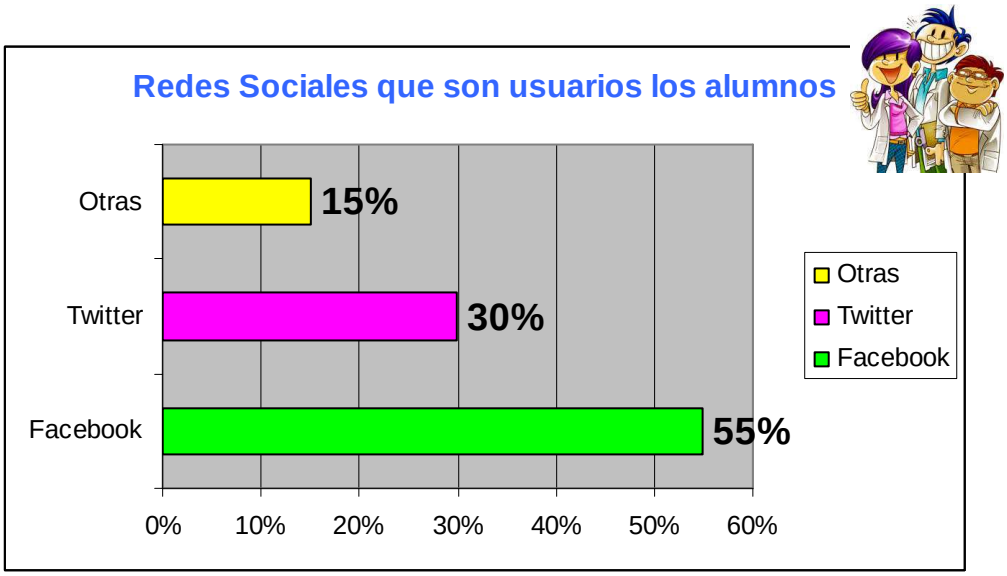


Ilustración 39- Redes sociales que son usuarios los alumnos.

La red social que llama más la atención de los adolescentes es Facebook que cuenta con el 55 % de los encuestados, por los diferentes servicios que ofrece a sus usuarios pero también son usadas otras redes sociales con menores porcentajes como Twitter que cuenta con el 30% y otras como Google+, Pinterest.

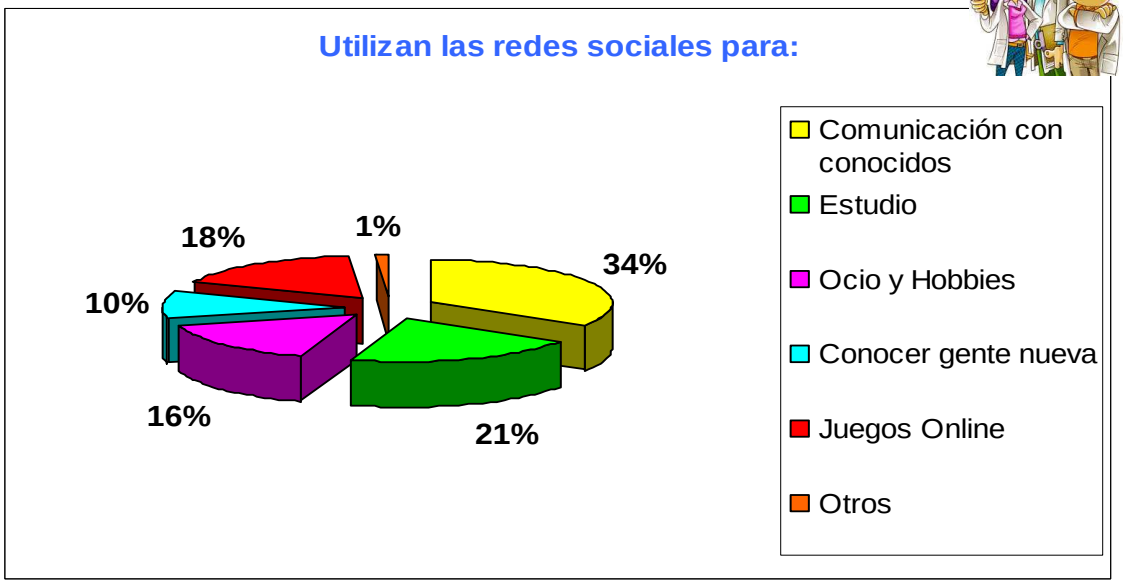


Ilustración 40- Utilización de las redes sociales

El 34 % de los alumnos utilizan las redes sociales para comunicarse con conocidos, el 21 % para estudiar, el 18 % para jugar en línea, 16 % para ocio y hobbies, el 10 % para conocer gente nueva.

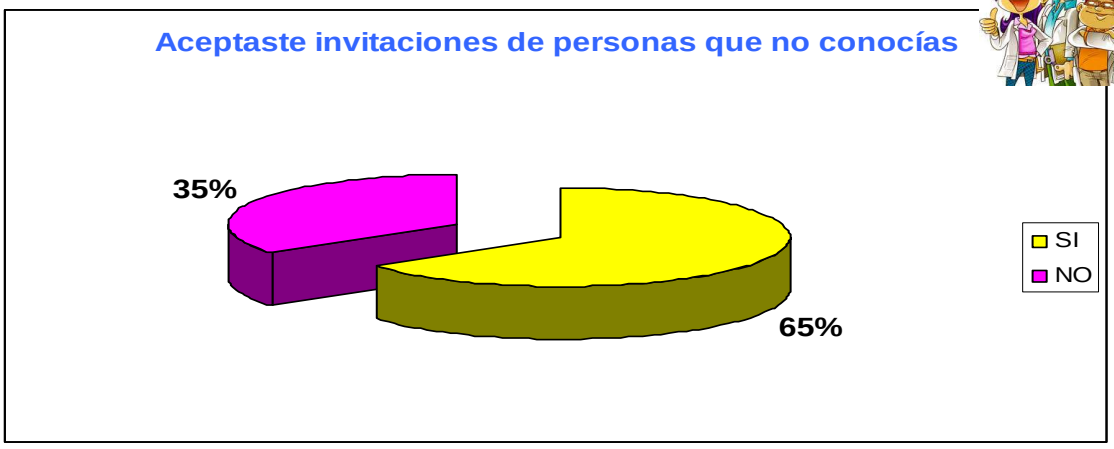


Ilustración 41- Porcentaje de aceptación de invitaciones de personas que no conocías.

El 65 % de los alumnos ha aceptado invitaciones de extraños.

Por ello debemos educar a nuestros adolescentes para que éstos desarrollen capacidades críticas y reflexivas respecto al uso de Internet y las nuevas tecnologías de información y comunicación, redes sociales. Y así puedan tener herramientas con que poder enfrentar las distintas amenazas que se le vayan presentando.

4.3. Privacidad en Sitios de Redes Sociales

Pertenecer a una red social (Facebook, Twitter, Pinterest, otras) tiene grandes ventajas pues en este tipo de sitios podemos encontrar a amigos, compañeros de trabajo, vecinos, en general gente que tiene intereses similares a los nuestros; además podemos compartir videos, fotografías, artículos y lo más importante podemos mantener comunicación con otras personas. Este tipo de servicios nos ayuda a mejorar nuestras relaciones con otras personas, pues podemos conocer un poco más acerca de nuestros amigos y familiares.

Desafortunadamente existen personas en los servicios de redes sociales que no tienen buenas intenciones, algunas de ellas buscan molestar a otros usuarios a través de ofensas o mensajes que pueden difamar a otra persona. Además en los sitios de redes sociales proporcionamos información que podría ser utilizada por algún delincuente para realizar robo de identidad, planear un secuestro o pasar del hostigamiento redes sociales a otros medios como correo electrónico, teléfono, SMS. Esto nos lleva a pensar en qué tipo de información debemos publicar y compartir con nuestros contactos en la red.

A continuación te damos algunas recomendaciones:

- No publiques información personal (teléfonos, correo electrónico, cuentas bancarias.). Normalmente este tipo de dirección la conocen nuestros amigos y familiares por lo que no es necesario publicarla en Internet.
- Establece restricciones a tu perfil. Los servicios de redes sociales permiten establecer restricciones sobre quién puede ver tu perfil y la información publicada (fotografías, comentarios), asegúrate que sólo tus amigos y las personas que conoces puedan acceder a esta información.

- Crea grupos de contactos y crea restricciones para cada uno de ellos. Algunos sitios de redes sociales permiten crear grupos para nuestros contactos, de tal modo que al crear un grupo podamos establecer permisos; por ejemplo si creamos el grupo Amigos y Contactos de trabajo nuestros amigos podrán ver ciertas fotografías y tendrán acceso a cierta información que nuestros Contactos de trabajo no podrán acceder.
- Procura ser selectivo al momento de aceptar contactos. Sabemos que el principal atractivo de las redes sociales es poder conocer a otras personas, sin embargo aceptar a cualquier persona como contacto puede ponernos en riesgo pues al aceptarlos damos ingreso a información confidencial y en muchas ocasiones desconocemos cuales son las intenciones de estas personas.

Ilustración 42. Peligros en las redes sociales.

- Lee las políticas de privacidad del servicio de redes sociales. Las políticas de privacidad de cada uno de los servicios establecen las reglas sobre qué puede hacer el servicio con nuestra información, es decir si se mantendrá como confidencial o si podrá enviarse a otros proveedores para que puedan contactarnos.

La mejor recomendación para seleccionar que información publicar o no, es seguir nuestro propio instinto, pues Internet es sólo una extensión a nuestra vida diaria, de tal modo que la información que no daríamos a un desconocido en la calle es la misma que debemos proteger en Internet.

Las entrevistas realizadas muestran que los alumnos tienen una escasa conciencia a cerca de la privacidad de sus datos, sólo el 31% de los alumnos configuró su privacidad y seguridad en las redes sociales. (Ver Ilustración 7).

A continuación proporcionamos una ayuda para la configuración de la privacidad y seguridad de las redes sociales más utilizadas por los alumnos encuestados Facebook y Twitter.

4.3.1. Alta como usuario en la red social Facebook

Ilustración 43- Alta de usuario en Facebook.

✓Facebook realiza una petición para importar todos los contactos desde la libreta de direcciones de correo.

✓Para ello, el usuario ha de introducir su contraseña de correo electrónico.

Facebook no almacena la contraseña de correo, pero sí la lista de contactos, a no ser que se especifique lo contrario.

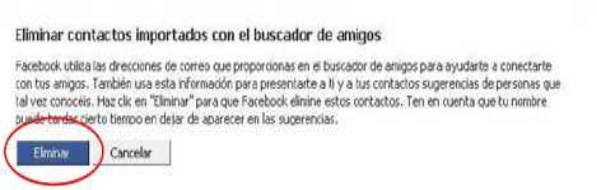


Ilustración 44- Alta de usuario en Facebook.

En la parte inferior de la web se encuentran tanto las Políticas de Privacidad de la plataforma como las Condiciones de Uso.

✓Si se accede a "Privacidad" el usuario se encuentra con "Guía sobre la privacidad en Facebook", la cual es una versión resumida y visual de cómo proteger la privacidad en la red social. Desde aquí se accede al documento propiamente dicho de Política de Privacidad.

✓La Política de Privacidad está en castellano y se desglosa en:

- ***Introducción***
- ***Información que recibimos***
- ***Información que compartes con terceros***
- ***Cómo utilizamos tu información***
- ***Cómo compartimos la información***
- ***Cómo puedes ver, modificar o eliminar información***
- ***Cómo protegemos la información***
- ***Otras condiciones***

Ilustración 45- Políticas de privacidad en Facebook.

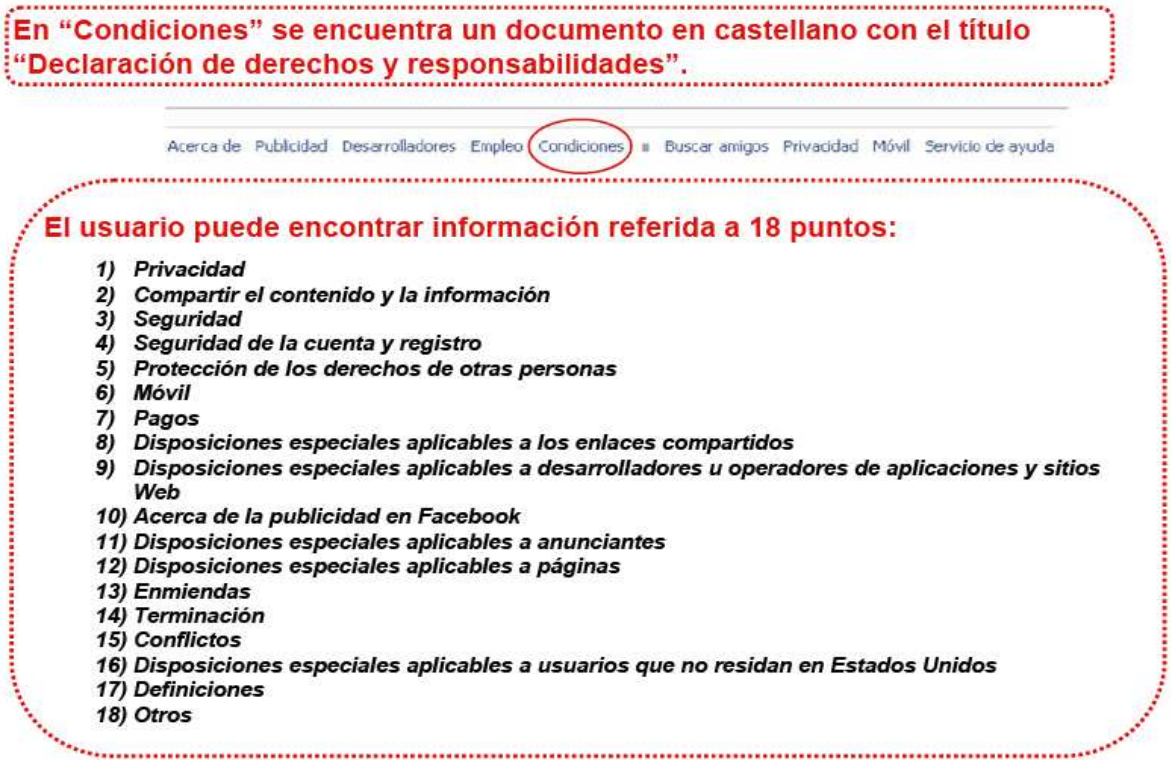


Ilustración 46- Políticas de privacidad en Facebook.

Participación en la red social.

Ilustración 47- Configuración de la privacidad en Facebook.

Ilustración 48- Información de perfil de usuario de Facebook.

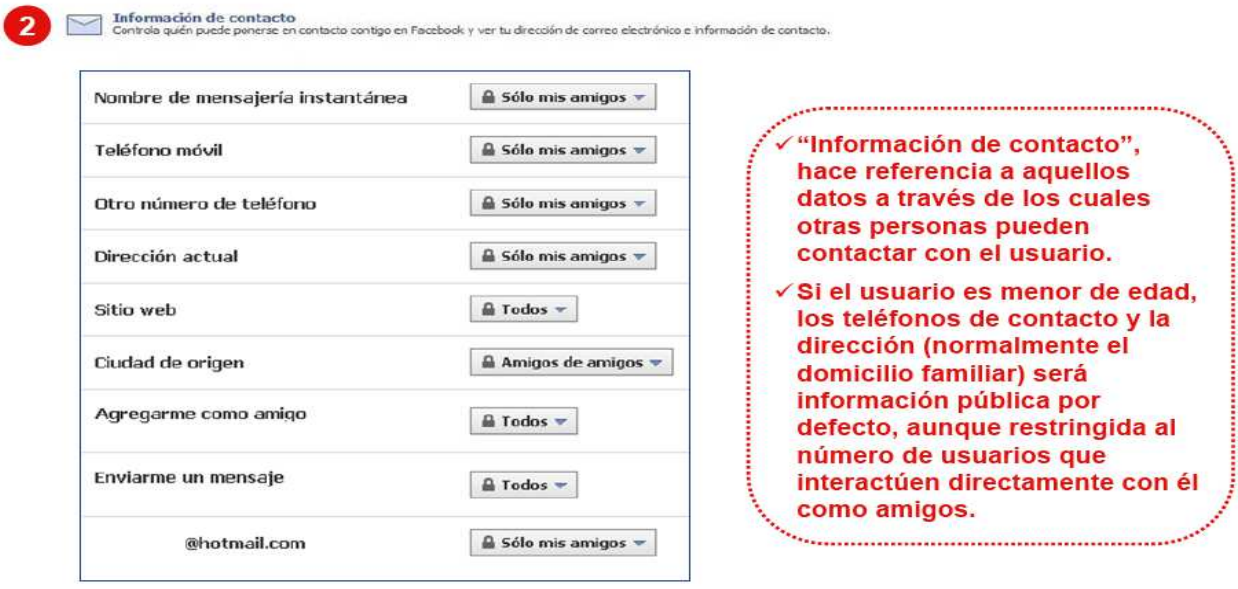


Ilustración 49- Información de contacto de Facebook.

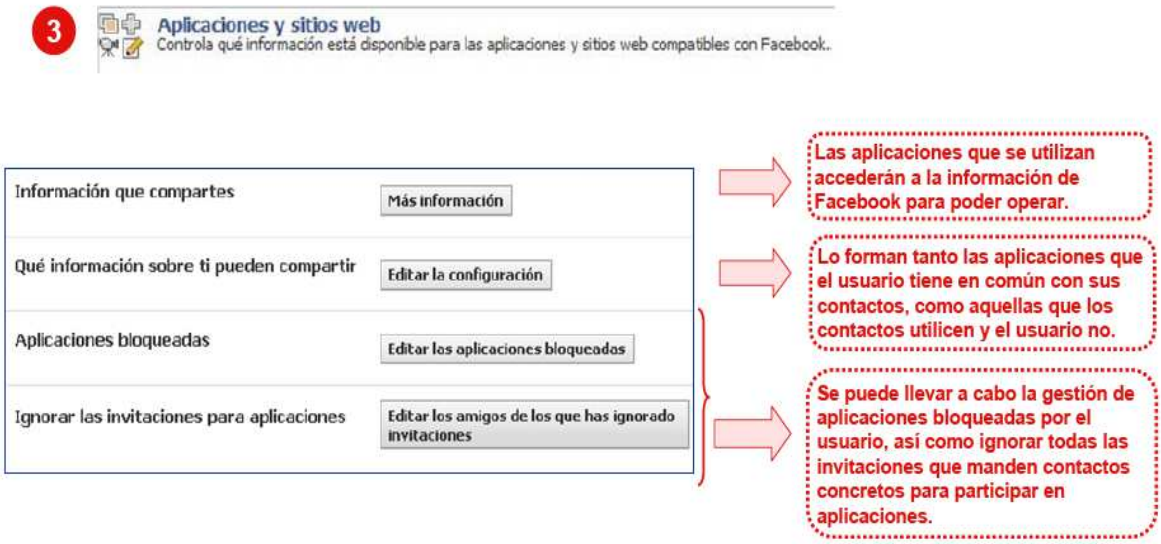


Ilustración 50- Aplicación y sitios Web de Facebook.

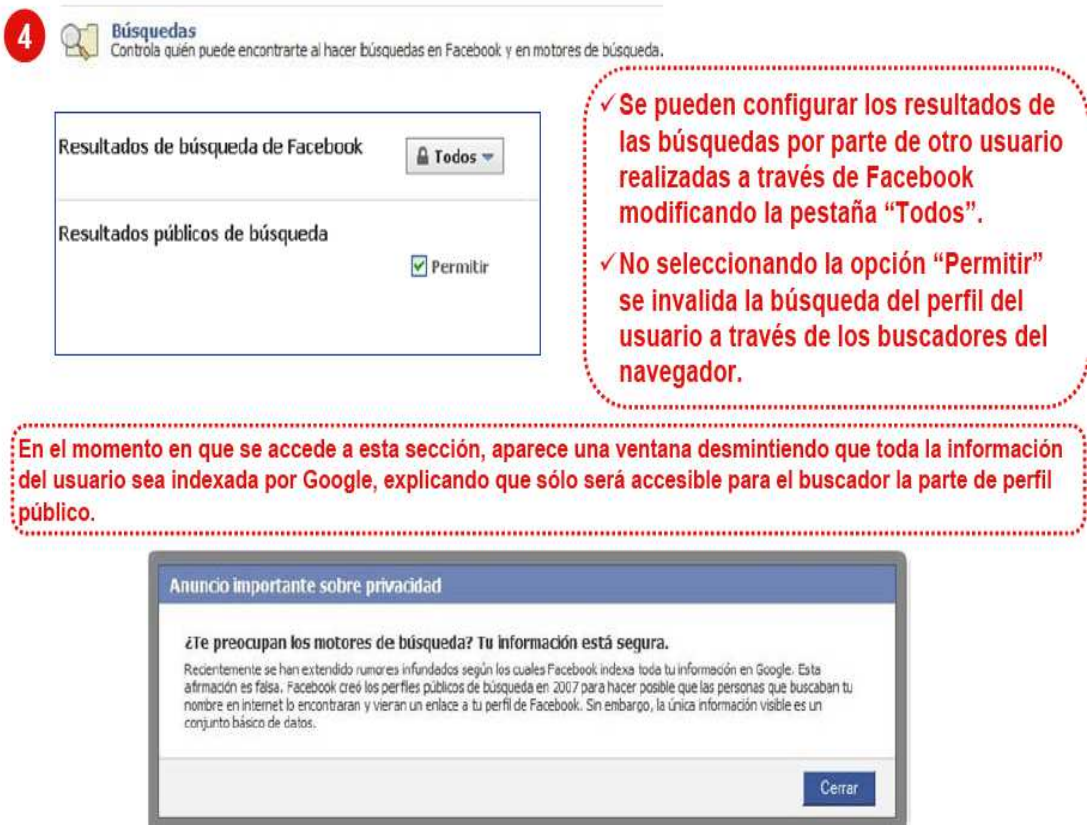


Ilustración 51- Búsquedas en Facebook.

Por último, se puede llevar a cabo la gestión de usuarios bloqueados. Es decir, se puede bloquear a aquellas personas que el usuario no desee que tengan contacto con él: no podrán enviarle mensajes, realizar "peticiones de amistad", ni ver su perfil. Se puede hacer de dos formas distintas:

- Especificando el nombre de la persona a bloquear.
- Especificando la dirección de correo electrónico.

Ilustración 52- Bloqueo en Facebook.

Propiedad intelectual

Respecto a la propiedad intelectual en las Condiciones de Uso se puede leer en el punto 2:

"Eres el propietario de todo el contenido y la información que publicas en Facebook (…). Para el contenido Protegido por derechos de propiedad intelectual, como fotografías y video (en adelante, 'contenido de PI'), nos concedes específicamente el siguiente permiso, de acuerdo con la configuración de privacidad y aplicaciones: nos concedes una licencia no exclusiva, transferible, con posibilidad de se sub-otorgada, sin royalties, aplicable globalmente, para utilizar cualquier contenido de PI que publiques en Facebook o en conexión con Facebook (en adelante, 'licencia de PI'). Esta licencia de PI finaliza cuando eliminas tu contenido de PI o tu cuenta, salvo si el contenido se ha compartido con terceros y éstos no lo han eliminado".

Publicación de fotografías

Ilustración 53- Propiedad intelectual en Facebook.

4.3.2. Baja del servicio de Facebook

Baja efectiva

Aunque se produzca la baja del usuario, la información de su cuenta no es eliminada de forma inmediata. Como indica la Política de Privacidad, lo que se solicita es la "desactivación de la cuenta", no su eliminación.

Conservación de los datos

La información referida a este aspecto es bastante ambigua:

"La información eliminada podría permanecer en copias de seguridad durante un tiempo razonable, pero generalmente no estará disponible para los miembros de Facebook".

Además recoge también:

"No nos hacemos responsables de que algún usuario burle las configuraciones de privacidad o las medidas de seguridad del sitio. Entiendes y aceptas que, incluso después de la eliminación de contenido perteneciente a un usuario, copias del mismo pueden permanecer visibles en páginas de memoria cache o archivadas o si otros usuarios lo han copiado o almacenado".

En las condiciones de uso, acerca de este tema, dice lo siguiente:

"Cuando eliminas contenido de PI (Propiedad Intelectual), este se borra de forma similar a cuando vacías la papelera o papelera de reciclaje de tu equipo. No obstante, entiendes que es posible que el contenido eliminado permanezca en copias de seguridad durante un plazo de tiempo razonable (si bien no estará disponible para terceros)".

Ilustración 54- Baja del servicio de Facebook.

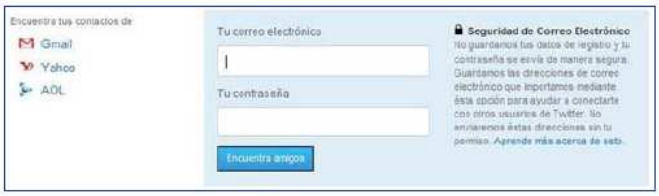
4.3.3. Alta de usuario en la red social Twitter

- ✓ **Twitter es una plataforma abierta a todo el mundo.**
- ✓ **Se trata de un espacio de microblogging donde publicar pequeños mensajes de estado que pueden incluir enlaces a sitios ajenos a la plataforma.**
- ✓ **Se solicitan pocos datos personales. Entre ellos no figura la edad ni fecha de nacimiento del usuario.**

- ✓ **Twitter no verifica la edad de sus usuarios durante el proceso de registro.**
- ✓ **Se realiza una comprobación de seguridad para así registros masivos.**

Ilustración 55- Alta como usuario en Twitter.

- ✓ **Existe la opción de buscar dentro de la red social a los contactos que el usuario tenga en su cuenta de correo de Gmail, Yahoo o AOL.**
- ✓ **Se solicita la contraseña de acceso a la cuenta de correo.**



- ✓ **Twitter no almacena los datos del usuario pero sí las direcciones de correo de los contactos que se importan.**
- ✓ **Dispone de una sección de ayuda para hacer búsquedas de usuarios por distintos medios.**

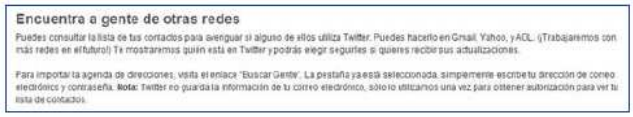


Ilustración 56- Alta como usuario en Twitter

En la parte inferior de la web se encuentran tanto las Políticas de Privacidad de Twitter como las Condiciones de Uso.

- ✓ **El documento de las "Condiciones de Uso" se presenta en español.**
- ✓ **El documento está constituido por 15 subapartados:**

1) ***Condiciones básicas***
2) ***Privacidad***
3) ***Contraseñas***
4) ***Contenido de los servicios***
5) ***Derechos del usuario***
6) ***Derechos de Twitter***
7) ***Restricciones en el contenido y uso de los servicios***
8) ***Política de derechos de autor***
9) ***Los Servicios están disponibles "AS-IS", (tal y como son y están disponibles actualmente)***
10) ***Enlaces***
11) ***Limitación de Responsabilidad***
12) ***Excepciones***
13) ***Cláusula de cesión y nulidad parcial***
14) ***Ley aplicable y jurisdicción competente***
15) ***Totalidad del acuerdo y convenio entre las partes***

Ilustración 57-Condiciones de uso de Twitter

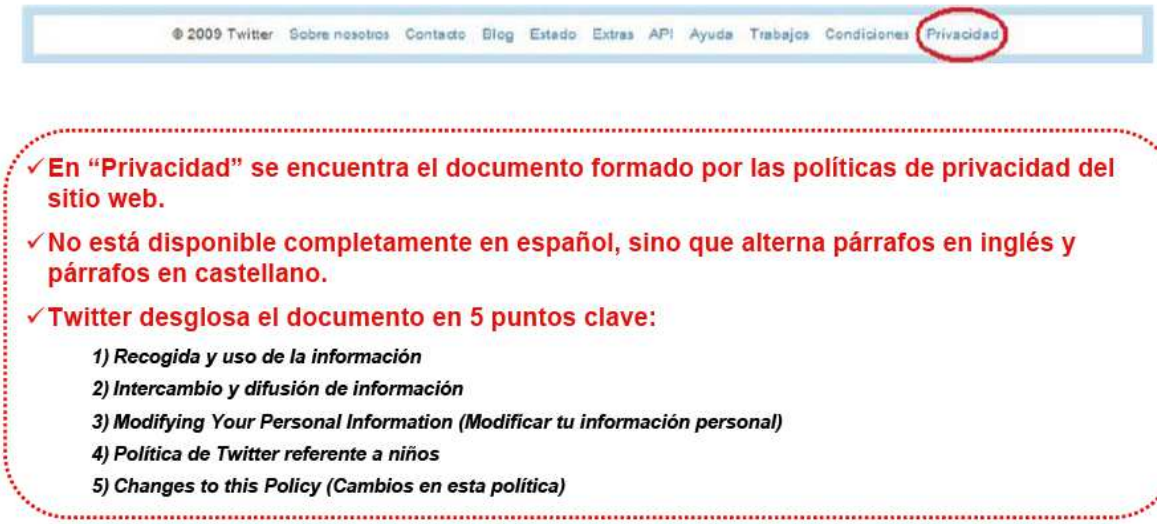


Ilustración 58- Privacidad en Twitter

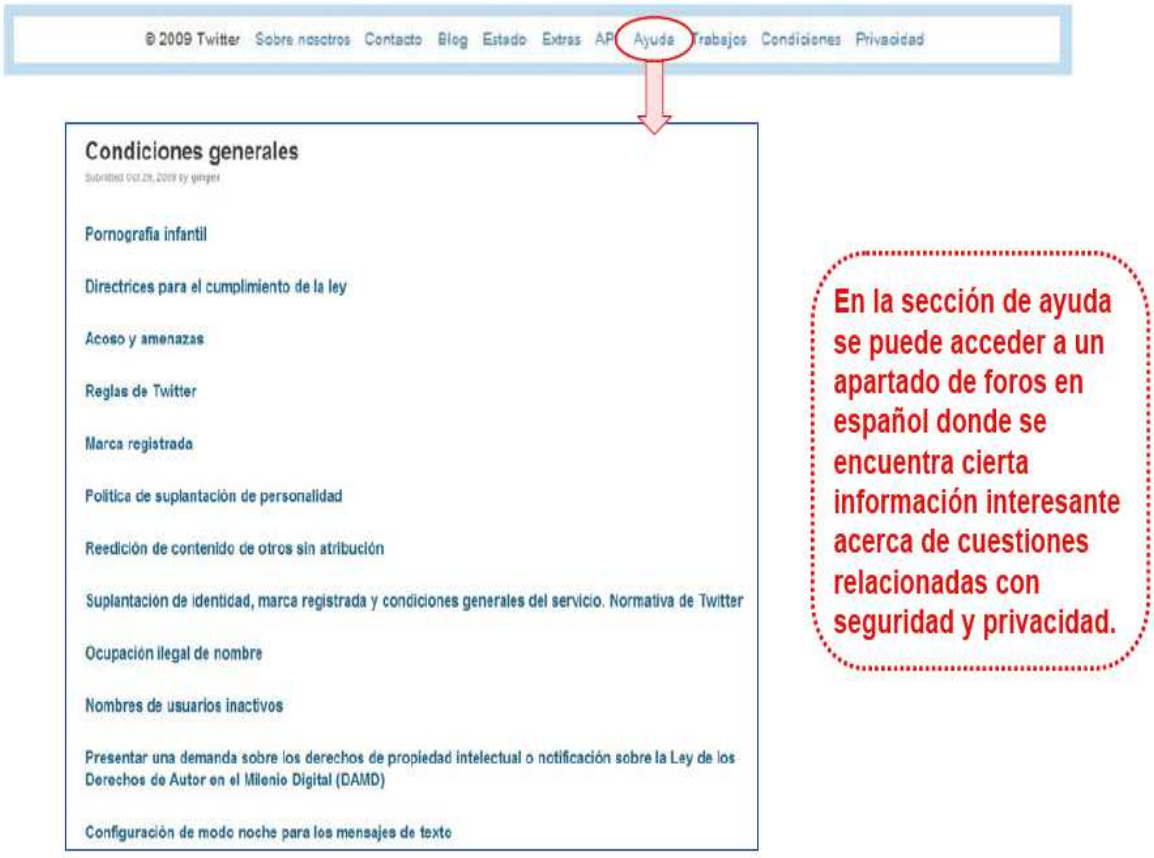


Ilustración 59- Condiciones generales de uso en Twitter

Participación en la red social Twitter

Ilustración 60- Configuración en Twitter

También se puede configurar si se desea recibir o no un correo electrónico del sistema.

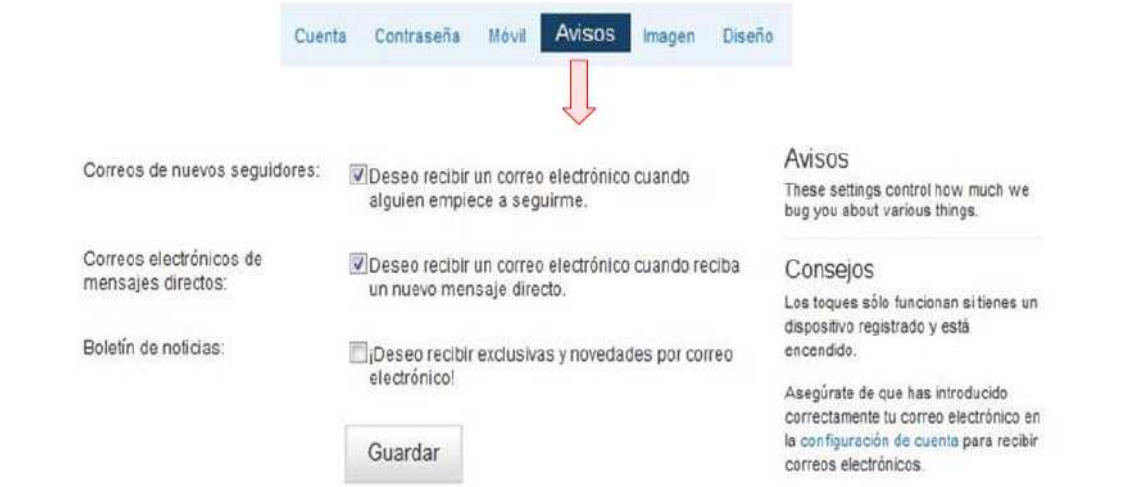


Ilustración 61- Configuración en Twitter

Propiedad intelectual

En lo referente a la propiedad intelectual, el usuario mantiene el derecho de propiedad del contenido pero proporciona a Twitter una licencia de uso del mismo, tal y como expone el documento de "Condiciones de Uso" del servicio:

> *"El usuario se reserva los derechos de cualquier contenido enviado, publicado o presentado a través de los Servicios. Al enviar, publicar o presentar cualquier Contenido a través de estos Servicios, el usuario otorga a Twitter licencia mundial, no exclusiva, libre de regalías (con derecho a la concesión de la licencia a terceros) para utilizar, copiar, reproducir, procesar, adaptar, modificar, publicar, transmitir, mostrar y distribuir dicho Contenido cualquier medio de comunicación o método de distribución (actual o desarrollado en un futuro)".*

También, habla del uso por parte de terceros asociados:

> *"El usuario acepta que este permiso otorga el derecho a Twitter de poner a la disposición de otras compañías, organizaciones o individuos asociados con Twitter del Contenido para la sindicación, difusión, distribución o publicación de dicho Contenido en otros medios y servicios, según a nuestros Condiciones generales para utilizarlo."*

Por otra parte, pone al servicio del usuario un sistema de notificación en caso de vulneración de los derechos de autor.

Ilustración 62- Propiedad intelectual en Twitter

Ilustración 63- Publicación de fotografías en Twitter

4.3.4. Baja del servicio de Twitter

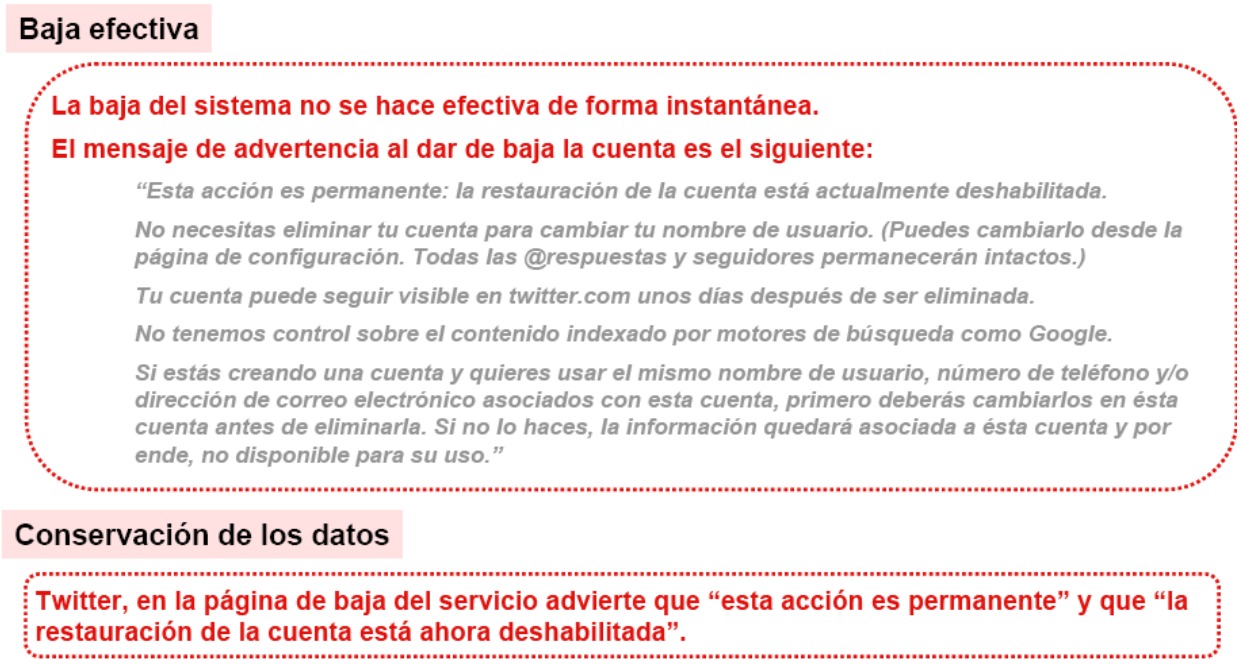


Ilustración 64- Baja del servicio de Twitter

Si un desconocido te solicita información personal en la calle,¿se la entregarías? Entonces tampoco lo hagas en la red.

No hables con extraños. Y, recuerda lo que ingresa a Internet jamás sale.

4.4. Juegos en Línea

Estas son algunas recomendaciones a tener en cuenta cuando juegas.

- Comportarse o hablar mal o hacer trampas no está bien. Puedes bloquear a los jugadores que hagan eso, notificar al proveedor del juego o contárselo a tus padres.
- Cuéntale enseguida a tus padres si te encuentras con información que te hace sentir incómodo.
- No des información personal, como por ejemplo la dirección de tu casa, tu número de teléfono o tu foto.
- Nunca te reúnas con nadie que conozcas en línea sin decírselo antes a tus padres.

Cuando navegas y juegas intenta utilizar alguna aplicación de Control Parental (cualquier herramienta que permita a los padres controlar y/o limitar el contenido que un menor puede utilizar en la computadora o accediendo en Internet) para que la misma controle los sitios a los que ingresas y su contenido. De esta forma te estarás protegiendo a ti mismo.

5. Concreción del Modelo

Llegamos a la instancia final del proyecto de grado, en la cual buscaremos lograr nuestro objetivo concientizar al usuario, por lo que se desarrolló un sitio Web y la planificación de un taller informativo, que genere un espacio de interacción entre alumnos, docentes y padres del Colegio San José, en base a lo desarrollado a lo largo de este proyecto.

Para el desarrollo de la aplicación Web se utilizó como plataforma Netbeans7.4, Html 5 y hojas de estilo en cascada o CSS.

A continuación se muestra la captura de pantallas de la Web con el fin de esclarecer la relevancia de la misma y el de su contenido. También, se anexa la planificación del taller (Anexo C).

Técnicas utilizadas para la recolección de información

Para llevar a cabo el relevamiento de información del caso de estudio, se utilizaron:

- *Encuestas*: se realizaron encuestas anónimas a todos los alumnos del nivel medio (Anexo A) y a los docentes (Anexo B) de la Institución. Durante el proceso de realización de las encuestas, hubo una gran predisposición por parte del cuerpo directivo, docentes y alumnos. De esta manera se pudo recoger información adicional y valiosa para la cumplimentación del proyecto.

5.1. Caracterización de la Institución

Ilustración 65- Fachada de la escuela

Nombre de la Institución: Colegio San José.

Tipo de Organización: Educativa.

Niveles: Inicial – Primario – Medio.

Orientación: Bachiller en Humanidades con Orientación en Ciencias Sociales.

Turno: Mañana y Tarde.

Idiomas: Inglés.

Domicilio: Madre Tránsito Cabanillas 350 – (5191) San Agustín – Córdoba.

Estructura Organizacional:

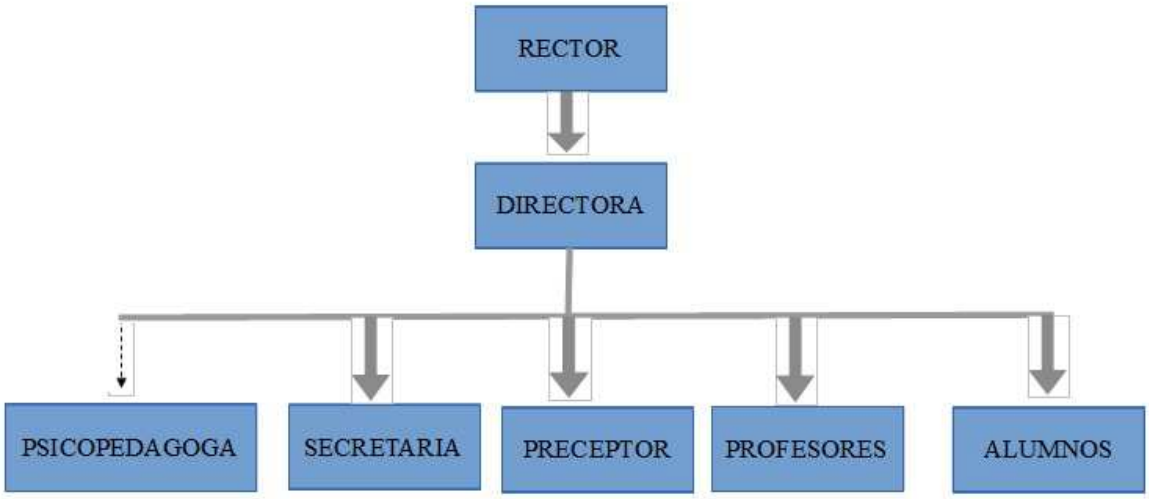


Ilustración 66 – Organigrama de la Institución Educativa

Los comienzos del Colegio San José se remontan al año 1916 cuando llegaron las Hermanas Terciarias Misioneras Franciscanas a un terreno donado por el Sr. Ing. Tristán Echenique, para que allí se erigiera una casa destinada a los retiros espirituales y del descanso. Desde aquel momento, y mientras se sucedían las actividades de construcción de dicha casa, las Hermanas fueron desarrollando nobles tareas de acompañamiento y de atención espiritual y educativa a muchas de los habitantes de San Agustín. Finalmente, en el año 1932 se fundó el colegio, siendo hasta el año 1989 un internado. Desde 1960 se abrió el nivel secundario, siendo su primera promoción en el año 1965.

A partir del año 2004, a Congregación tuvo que retirar la Comunidad Religiosa del lugar, comenzando una experiencia de Misión Compartida. Por ello el colegio es gestionado por un grupo de laicos, con el acompañamiento atento y cariñoso de la Congregación de Hermanas Terciarias Misioneras Franciscanas, que sigue comprometida con la tarea encomendada por Madre María del Tránsito, de “llevar el precioso contingente de la fe, a los pueblos pobres de la República”.

La Congregación de Hermanas Terciarias Misioneras Franciscanas posee la Casa Madre en Córdoba Capital, el resto de Colegios se extienden a lo largo de todo el país. A continuación, éstos se pueden ver en la ilustración:

Casas de las Congregaciones:

Ilustración 67– Congregaciones en Argentina

FECHAS FUNDACIONALES DE LAS CASAS DE LA CONGREGACIÓN

1° 08-12-1878: Casa Madre - Colegio Santa Margarita de Cortona – Córdoba
2° 02-07-1879: Colegio Nuestra Señora del Carmen - Río Cuarto – Córdoba
3° 19-03-1882: Colegio Inmaculada Concepción - Villa Nueva – Córdoba
4° 17-09-1887: Colegio Santa Rosa de Viterbo – Salta
5° 03-02-1901: Colegio San Antonio - Villa María – Córdoba
6° 19-03-1901: Colegio El Transito de Nuestra Señora - San Juan
7° 03-03-1907: Colegio Nuestra Señora de Lourdes - Banfield – Bs. As.
8° 04-03-1917: Colegio Nuestra Señora de Itatí - Resistencia – Chaco
9° 08-03-1925: Colegio Heguy de la Sagrada Familia - Intendente Alvear – La Pampa
10° 19-03-1925: Colegio Castro Barros San José - Lucas González – Entre Ríos
11° 30-05-1931: Residencia Santísima Trinidad - Agua de Oro – Córdoba (el 19-03-2010 se funda la Casa de Oración Santísima Trinidad)
12° 01-01-1933: Colegio San José - San Agustín – Córdoba
13° 09-06-1941: Casa de descanso La Choza - Salta (el 08-12-1970 Casa de Retiros La Choza)
14° 19-03-1959: Colegio Nuestra Señora de Guadalupe - Calchaquí - Santa Fe
15° 09-06-1963: Casa Generalicia Inmaculada Concepción – Córdoba
16° 02-02-1970: Colegio Maria Reina - Santiago – Chile
17° 1973: Residencia de ancianas Niño Jesús - Santiago – Chile
18° 22-08-1999: Enfermería Santa Clara (Ubicada en Casa Generalicia - Córdoba)
19° 18-05-1993: Residencia Misionera Madre Mª del Transito - Joaquín V. González - Salta
20° 02-03-2008: Comunidad Inmaculado Corazón de Maria - Hospital San Juan Bautista - Santo Tomé – Corrientes

Actualmente el Colegio San José, es una pequeña comunidad educativa mixta, integrada por 160 alumnos en el nivel Medio y aproximadamente 25 docentes.

Entre nivel Inicial y Primario, cuenta con 200 alumnos aproximadamente, mientras que los maestros son 12.

5.2. Página Web

La página de inicio de nuestra Web se visualiza de la siguiente manera:

Ilustración 68- Página Inicio de la Web.

En el margen superior, se observan tres imágenes (alumnos, padres, docentes) permitiendo cada una de ellas acceder al espacio correspondiente.

Debajo de las figuras, se encuentra un que nos permite acceder a información sobre Ingeniería Social.

La página se divide en dos partes: a la izquierda, una imagen y el logo del colegio, que referencia al portal Web de la Institución; a la derecha, la portada de Bienvenida.

En la parte inferior de la página, se visualizan noticias de la actualidad relacionadas con la Ingeniería Social.

Sección ALUMNOS:

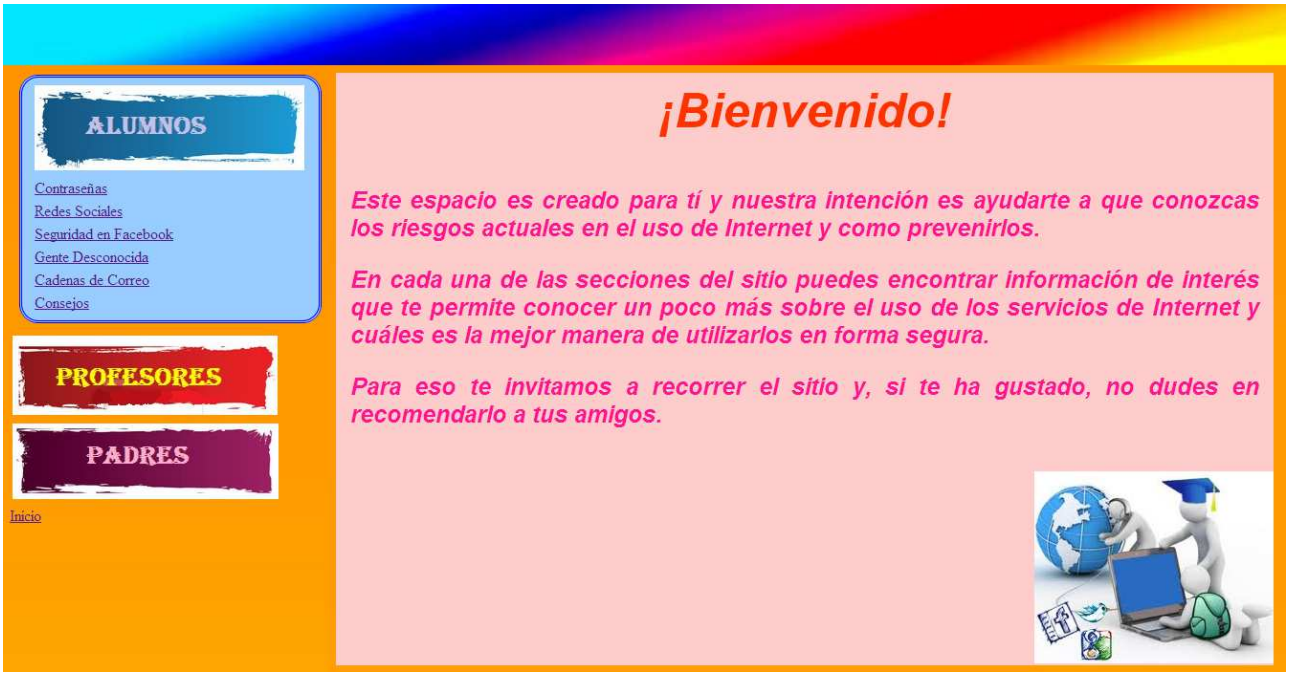


Ilustración 69– Sección Alumnos

Como lo muestra la pantalla, a la izquierda se encuentra el submenú de ALUMNOS, pudiendo ir los submenús de PROFESORES o PADRES o volver al Inicio de la página.

Submenú ALUMNOS:

Ilustración 70– Submenú alumnos

Dentro de cada uno de estos vínculos se detallan: tutoriales, ventajas, desventajas, configuraciones para mejorar la seguridad y evitar la violación de la privacidad, consejos. Se exponen videos y/o noticias ilustrativas y actividades.

Submenú PROFESORES:

Ilustración 71- Submenú profesores

Dentro de cada uno de estos vínculos se suministra información de utilidad para los docentes, de la que pueden hacer uso junto a los alumnos. Se anexa

material extra que puede ser consultado por los docentes y se presentan estadísticas que proveen información relevante de lo expuesto que están los adolescentes frente a los ataques de la Ingeniería Social.

Submenú PADRES:

Momentáneamente se encuentra en construcción, aunque pensamos integrarlos en el futuro a este desafío: la concientización del usuario frente al uso de Internet.

6. Conclusión

A lo largo de este proyecto se realizaron encuestas y el resultado de dichas encuestas, arrojaron estadísticas que demostraron la escasez de conocimientos que poseen los alumnos y docentes de la Institución sobre la Ingeniería Social y sus implicancias. Esto nos dio un punta pie inicial para abordar esta investigación. En resumen, los resultados obtenidos de las encuestas obtuvimos las siguientes conclusiones:

- Todos los adolescentes utilizan Internet con distintos fines.
- Un alto porcentaje de adolescentes, 85 % nunca escucho hablar de Ingeniería Social, esta falta de información vuelve a los adolescentes más vulnerables y los deja expuesto a los riesgos que esto conlleva
- Se conectan a Internet frecuentemente y el 50% lo hace desde su casa.
- Un elevado porcentaje de adolescentes son usuarios de alguna red social (la mayoría del Facebook y Twitter).
- Las redes sociales ofrecen diversas funcionalidades como: de medio de comunicación, espacio para conocer gente nueva, interaccionar con amigos, familia conocidos y desconocidos, las redes sociales son un lugar en el que se puede compartir documentos, fotos, videos y otros.
- Lo más preocupante, es que el 69 % cree que sus datos están seguros en las redes sociales y el 65 %, ha aceptado invitaciones de personas desconocidas.
- La mayoría de los adolescentes es usuario de correo electrónico y utiliza correo electrónico, de los cuales 76 % alguna vez a recibido correo electrónico promocionando servicios no solicitados y el 53 % abrieron dichos correos.
- El 11% comparte sus contraseñas con amigos, esto indica que un pequeño porcentaje no tiene sus contraseñas protegidas y no son privadas.
- El 91% de los docentes nunca escuchó hablar de Ingeniería Social. El 94% de los docentes están dispuestos a conocer más acerca del tema.

- Los docentes están dispuestos a apoyar a las tesistas para alcanzar el objetivo del presente proyecto de grado, manifestando que sí les gustaría planificar una clase abordando el tema de la Ingeniería Social, en la que utilizarían como soporte la página Web.
- A diferencia de los adolescentes, los docentes utilizan frecuentemente el correo electrónico. Mientras que los jóvenes prefieren el celular para conectarse a Internet, los adultos lo hacen desde notebooks o computadoras personales (PC).
- Al igual que sus alumnos, utilizan redes sociales y la mayoría son usuarios de la red social Facebook.
- Una pequeña proporción de docentes utiliza las redes sociales como vía de comunicación con sus alumnos para fines educativos (proporcionar material didáctico).
- Muchos docentes utilizarían las redes sociales para el intercambio de información y desarrollo de proyectos en común con otros colegas, un breve porcentaje utilizaría las redes sociales para trabajar con sus alumnos.
- Mediante las redes sociales los adolescentes se vuelven fáciles víctimas de personas que se dedican a actividades peligrosas como: falsificación de identidad o violación de la privacidad, ya que a través de una pantalla es posible que estas personas mientan acerca de su identidad presentándose como un adolescente más.

A lo largo de este proyecto se realizaron investigaciones de distintas fuentes. Visualizando en todo momento, lo vulnerable que están los usuarios frente a las amenazas de los ingenieros sociales.

Se desarrolló una sitio Web, con información, consejos, videos. Como una manera de llegar a la comunidad educativa. Además, se deja planteado como solución a futuro la ejecución de talleres informativos en la Institución Educativa, utilizando la página Web desarrollada para informar los usuarios y educarlos con herramientas para que puedan defenderse y estar alertas. Contando con el respaldo de los directivos y profesores quienes en todo momento tuvieron la mejor

predisposición hacia con nosotras. Demostrando estar interesados en este tema y en la problemática en general que están sufriendo los adolescentes con el uso de las nuevas tecnologías de información y comunicación, y redes sociales.

Para finalizar podemos aseverar, que la Ingeniería Social es una de las nuevas formas de los atacantes y estafadores a nivel electrónico y a nivel personal. Este es un problema grave de información ya que no se cuenta con lo requerido para poder frenar a estos “Ingenieros Sociales”. No se trata solamente de proteger nuestro hardware. Se debe estar informado de todos los métodos que utilizan, ya que por una simple invitación de amistad en la red social Facebook, se puede ser vulnerable al ataque. Para poder evadir estos ataques es necesario estar ***informados***, ya que hasta el anuncio mas insignificante y pequeño puede ser el que desate una ola de problemas a los cuales nos tendremos que enfrentar en un futuro y a sus implicaciones en nuestra vida diaria, una simple solicitud de amistad podría ser, la causa de nuestra bancarrota o peor aun, podría destruir nuestra reputación.

Por ello debemos educar a nuestros adolescentes para que éstos desarrollen capacidades críticas y reflexivas respecto al uso de Internet y las nuevas tecnologías de información y comunicación y redes sociales. Y así puedan tener herramientas con que poder enfrentar las distintas amenazas que se le vayan presentando.

7. Referencias Bibliográficas

1. Taller de Ethical Hacking- Capacitación IT- Septiembre 2013.

2. Carracedo Gallardo, Justo – Seguridad en redes telemáticas – Mc Graw Hill 2004.

3. Apuntes Diseño Web avanzado (Html .5 y Css. 3) - Academia Santo Domingo.

4. Kevin D. Mitnick & William L. Simon. The Art of Deception: Controlling the Human Element of Security 1st. John Wiley & Sons, Inc., New York, NY, USA ©, 2002. ISBN 0-7645-4280-X.

5. Kevin D. Mitnick & William L. Simon. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers. Wiley Publishing, Inc., 2005. ISBN 0-7645-6959-7.

6. http://www.social-engineer.org/http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

7. http://en.wikipedia.org/wiki/Social_engineering_(security)#Techniques_and_terms

8. http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf

9. http://www.infospyware.com/articulos/que-es-el-phishing/

10. Internet Sano- Eset.

11. https://www.argentinacibersegura.org/materiales.php

12. http://www.lavoz.com.ar/sucesos/enganada-por-facebook-casi-sufre-calvario

13. http://peritoit.com/2013/01/28/el-fraude-a-traves-de-internet-unas-cifras-y-tendencias-orientativas/

14. http://www.enter.co/cultura-digital/redes-sociales/policia-encubierto-en-facebook-da-una-leccion-a-adolescentes/

15. Material sobre escuela y medios. Ministerio de Educación – Septiembre 2010.

16. Libro “Influencia, la psicología de la persuasión”- Dr. Robert B Cialdini- profesor de la Universidad Estatal de Arizona.

17. Informe de “El fraude a través de Internet”, Inteco (Instituto Nacional de la Tecnología y la Comunicación) año 2013.

18. http://www.mariadeltransito.org.ar/san_jose.html

19. Monográfico – Redes Sociales – Historia de las Redes Sociales. Ministerio de Educación, Cultura y Deporte. España.

ANEXO A

Encuesta realizada a los alumnos.

Encuesta de Ingeniería Social al Colegio San José

Sexo

- ☐ Masculino
- ☐ Femenino

Edad

¿Has escuchado hablar de Ingeniería Social?

- ☐ SI
- ☐ NO

¿Utilizas Internet?

- ☐ SI
- ☐ NO

¿Con qué frecuencia utilizas Internet?

- ☐ Nunca
- ☐ De vez en cuando
- ☐ Frecuentemente

¿Desde qué dispositivo te conectas a Internet?

- ☐ Computadora Personal
- ☐ Celular
- ☐ Tablets
- ☐ Notebook
- ☐ Otros:

¿Desde qué lugar te conectas a Internet?

- ☐ Desde tu hogar
- ☐ Desde el colegio
- ☐ Otros:

¿Utilizas correo electrónico?

- ☐ Nunca
- ☐ De vez en cuando
- ☐ Frecuentemente

¿Cuál de los siguientes requisitos incluyes en tu contraseña?

- ☐ Números
- ☐ Más de 10 caracteres

- ☐ Mayúsculas
- ☐ Signos especiales
- ☐ Combinación de alguna de las anteriores
- ☐ Otros:

¿Compartes tu contraseña con amigos?

- ☐ SI
- ☐ NO

¿Recibiste correos electrónicos que promocionaban servicios no solicitados?

- ☐ SI
- ☐ NO

En caso que sea SI, la respuesta anterior ¿Visitaste dichas páginas?

- ☐ SI
- ☐ NO

¿Eres usuario de las Redes Sociales?

- ☐ SI
- ☐ NO

¿De qué Redes Sociales eres usuario?

- ☐ Facebook
- ☐ Twitter
- ☐ Otros:

¿Qué tan seguro crees que están tus datos en los servidores de Redes Sociales?

- ☐ Seguros
- ☐ Inseguros

¿Para qué utilizas las Redes Sociales?

- ☐ Comunicación con conocidos
- ☐ Estudio
- ☐ Ocio y Hobbies
- ☐ Conocer gente nueva
- ☐ Juegos online
- ☐ Otros:

¿Aceptaste invitaciones de amistad de personas que no conocías?

- ☐ SI
- ☐ NO

ANEXO B

Encuesta realizada a los docentes.

Encuesta para profesores del Colegio San José

Agradecemos de antemano su colaboración.
Materia que dictas

¿Qué edad tienes?

- ☐ Menos de 25 años
- ☐ 25- 30 años
- ☐ 31- 40 años
- ☐ 41- 50 años
- ☐ 51- 60 años
- ☐ Mayor de 61 años

Sexo

- ☐ Femenino
- ☐ Masculino

¿Ha escuchado hablar sobre la Ingeniería Social?

- ☐ SI
- ☐ NO

¿Estaría dispuesto a conocer más sobre Ingeniería Social aplicada a las nuevas tecnologías y sus consecuencias?

- ☐ SI
- ☐ NO

¿Le gustaría planificar una clase en su materia integrando el tema de Ingeniería Social aplicada a las nuevas tecnologías, con apoyo de una página Web que contiene toda la información sobre Ingenieria Social?

- ☐ SI
- ☐ NO

¿Utiliza Internet?

- ☐ Nunca
- ☐ De vez en cuando
- ☐ Frecuentemente

¿Desde qué dispositivo se conecta a Internet?
Puede elegir más de una respuesta

- ☐ Computador Personal
- ☐ Celular
- ☐ Tablet
- ☐ Notebooks

- [ ] Otros:

¿Utiliza correo electrónico?

- [ ] Nunca
- [ ] De vez en cuando
- [ ] Frecuentemente

¿Cuál de los siguientes requisitos incluye en su contraseña?
En caso de utilizar correo electrónico.

- [ ] Números
- [ ] Más de 10 caracteres
- [ ] Mayúsculas
- [ ] Signos especiales
- [ ] Combinación de alguna de las anteriores
- [ ] Otros:

¿Utiliza el correo electrónico como vía de comunicación con sus alumnos?

- [ ] SI
- [ ] NO

¿Qué tipo de información usted transfiere con su alumnado por correo electrónico?
En caso de ser positiva la respuesta anterior.

- [ ] Fecha de exámenes
- [ ] Apuntes /Material didáctico
- [ ] Actividades escolares
- [ ] Otros:

¿Cuál de estas redes sociales utiliza?
Puede elegir más de una respuesta

- [ ] Facebook
- [ ] Twitter
- [ ] Linkedin
- [ ] Ninguna
- [ ] Otros:

¿Cual sería la/las utilidades que usted le daría a las redes sociales?
Puede elegir más de una respuesta

- [ ] Creación de una comunidad de profesores con intereses compartidos
- [ ] Intercambio de información (ideas, recursos, etc.)
- [ ] Desarrollo de proyectos comunes con otros docentes
- [ ] Trabajo con alumnos
- [ ] Otros:

¿Utiliza las redes sociales como vía de comunicación con sus alumnos?

- [ ] SI
- [ ] NO

¿Qué tipo de información usted transfiere con su alumnado en las redes sociales?
En caso de ser positiva la respuesta anterior

- [ ] Fecha de exámenes

- ☐ Actividades/ Material didáctico
- ☐ Actividades Escolares
- ☐ Otros:

ANEXO C

Planificación del Taller

TALLER: Ingeniería Social

Presentación

En el campo de la Seguridad Informática, la Ingeniería Social se conoce como la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos.

Podemos definir Ingeniería Social como el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros.

La Ingeniería Social se sustenta en el principio de que en cualquier sistema *"los usuarios son el eslabón más débil"*.

La Ingeniería Social está viviendo un verdadero auge, alentada por algunos factores en crecimiento como lo tecnológico, la movilidad, conectividad y redes sociales. Sin duda este crecimiento, favorece a las técnicas orientadas al engaño.

En esta propuesta informativa se procura presentar información valiosa, mostrando usos, ventajas, desventajas, configuraciones, estrategias y casos actuales de violación de privacidad, para que empecemos a tomar conciencia y utilizar Internet de forma segura y responsable.

Modalidad: Presencial

Duración: Un mes.

Forma de Cursado: día y horarios a convenir con la Institución.

Destinatarios: docentes, directivos, alumnos y padres del nivel medio.

Objetivos:

- Conocer qué es la Seguridad Informática, qué es Ingeniería Social y cuáles son sus técnicas.
- Adquirir conocimientos fundamentales relativos a la importancia del estudio de la Ingeniería Social.
- Conocer qué son y para qué sirven las Redes Sociales.
- Conocer la relación Redes Sociales e Ingeniería Social.
- Conocer y utilizar herramientas y estrategias para minimizar los riesgos al utilizar Internet y sus servicios: chat, email, redes sociales, otros.
- Administrar los dispositivos tecnológicos de manera segura y responsable.
- Adquirir conocimientos fundamentales relativos a la temática, para concientizar a los usuarios (alumnos, profesores, padres y a la comunidad educativa en general).

Contenido

Clase 1:

- Introducción a la Seguridad Informática.
- Concepto y técnicas de Ingeniería Social.
- Conociendo el sitio Web.
- Uso seguro y responsable de Internet.
- Internet en las aulas y en el hogar.

Clase 2:

- Concepto de redes sociales.
- Relación redes sociales – Ingeniería Social.

- Políticas de privacidad.
- Configuraciones de redes sociales.
- La privacidad online.

Clase 3:

- Navegación segura.
- Cómo crear contraseñas seguras.
- Control parental.
- Necesidades e importancia de la privacidad online.
- Configuraciones de correo electrónico.

Clase 4:

- Información y consejos para la prevención.
- Principales redes sociales, semejanzas y diferencias.
- Recomendaciones para docentes, padres y alumnos.
- Análisis de casos puntuales.

Coordinación y Equipo de capacitación

A cargo de las autoras del presente proyecto.

Materiales

- Sitio Web.

- Presentaciones en Power Point.
- Se permite el uso de dispositivos tecnológicos.
- Videos, para su posterior análisis.
- Todo material didáctico que favorezca el desarrollo de este proyecto.