Ciudadela
CIENTÍFICA
Cursos de Internet
para todas y todos

CURSO EN SEGURIDAD Y DELITOS INFORMÁTICOS

TEXTO DE APOYO AL ESTUDIANTE

GOBIERNO AUTÓNOMO DEPARTAMENTAL DE COCHABAMBA

Cochabamba tierra bendita

Curso en Seguridad y delitos informáticos
Programa en Alfabetización digital - Internet para Todas y Todos
Gobernación de Cochabamba
Manual de capacitación

Contenidos

Este texto pertenece a:

_____

1. Introducción

1.1. Bienvenida al Curso

Estimado y estimada participante, estamos muy complacidos que esté tomando este curso de Seguridad y delitos digitales. Este manual está pensando para que te guíe a lo largo del curso, en él encontrarás todo lo que abordaremos en estas 10 horas de capacitación y te servirá para futura referencia. Las clases no pretenden ser un espacio donde la única que habla es la facilitadora, por lo que te pedimos que ante cualquier duda levantes la mano y hagas comentarios, preguntas o sugerencias.

No existen preguntas malas ni buenas, igualmente, estaremos felices de ayudarte en lo que sea que necesites. Las clases pretenden ser lo más prácticas posibles, pues creemos que la mejor forma de aprender es haciendo, con casos de la vida cotidiana a los que nos enfrentamos todos.

Si crees que algo puede mejorarse, falta o quieres que se profundice más, no dudes en acercarte a cualquier persona del equipo, estamos dispuestos a ampliar cualquier información, absolver cualquier duda o incluso modificar y/o ampliar los contenidos presentados.

Sin más que decir, bienvenido/bienvenida al curso de Seguridad y delitos digitales.

1.2. ¿Por qué es importante este curso?

En los últimos años el acceso a Internet en nuestro país se ha disparado, en el año 2015, aproximadamente el 40% de las personas en Bolivia se conectaba a Internet con regularidad; para el año 2017 esta cifra aumentó hasta el 67,5%, más de 20 puntos porcentuales en sólo 2 años. Para Cochabamba, el dato actual nos indica que el 64% de la población de todo el departamento se conecta a internet.

Por esto creemos que es momento de empezar a preocuparnos acerca de cómo se están usando las TIC y los riesgos a los que la población está expuesta.

1.3. Certificación y reglas de juego

Acerca de la certificación, será avalada por el Gobierno Autónomo Departamental de Cochabamba, la UCATEC y la UNIVALLE. Cualquiera de los cursos que concluyas te hará acreedor a un certificado por 10 horas de taller.

Para poder gozar de un certificado es necesario que asistas al 100% de la capacitación en la que te has inscrito.

Existe una tolerancia de 15 minutos para contar tu asistencia, si cuando llegues la clase ha iniciado te rogamos que ingreses al aula en silencio y sin saludar, para no interrumpir.

Los facilitadores necesitan acreditar que la persona que se inscribió es la misma que asistió al curso, por lo que la primera sesión se te solicitará presentar tu carnet de identidad. Por favor no lo olvides.

En el curso debe primar el respeto, estamos muy abiertos a cualquier crítica, comentario, pregunta, declaración, siempre y cuando se haga sin interrumpir el normal desarrollo de la clase y, principalmente, sin ofender, atacar o insultar a ninguno de los asistentes, facilitadores, apoyos o cualquier persona en general. No se permiten actitudes sexistas, racistas o clasistas.

2. Datos, delincuencia informática y el negocio de la ciberseguridad

2.1. ¿Qué son los datos personales?

En internet se generan varios tipos de datos. Están, por un lado, los datos que los usuarios registran voluntariamente a través del llenado de formularios de registro para obtener una cuenta de correo o alguna cuenta en una plataforma de redes sociales, los datos que se dejan al usar los sitios de banca en línea, de compra por internet y otros que proveemos conscientemente. Por el otro, están los datos que se generan a través de la propia navegación y de los cuales no somos conscientes, reciben el nombre de “metadatos”, y son aquellos que se registran automáticamente al hacer clic en una página, al realizar una búsqueda, al subir una foto a Facebook, etc. Estos metadatos indican, por ejemplo, el lugar desde donde hiciste la acción, la hora, el dispositivo que usabas, el sistema operativo, a quién se lo enviaste, entre otros aspectos. Todos estos datos, pueden revelar información personal del usuario.

Para entender mejor qué son los metadatos y las implicaciones en los derechos digitales, les invitamos a ver el video de Red de Defensa de los Derechos Digitales (R3D), ONG mexicana https://www.youtube.com/watch?v=iKccR3E6jn4

Entonces, los datos personales son cualquier información referente a las personas/usuarios que puedan ayudar a identificarlos (nombre, número de carnet de identidad, dirección, teléfono, correo electrónico, etc.) a localizarlos, o que describan aspectos personales (cantidad de dinero en la cuenta bancaria, preferencia sexual, auto-identificación étnica, gustos de compra, situación laboral, situación amorosa, etc.). Estos datos son valiosos para las personas y pueden tener cierta sensibilidad, pero también son valiosos para empresas, gobiernos y, sobre todo, para delincuentes.

2.2. ¿Cómo se benefician de tus datos personales?

Las empresas se benefician de estos datos pues pueden segmentar mejor su marketing y bombardear de publicidad a los usuarios, incluso presionar con sus algoritmos de

búsqueda para que cierto tipo de consumo incremente, refleje o no una necesidad de la ciudadanía. Les resulta útil saber si la persona tiene gustos por un particular tipo de zapato, si piensa viajar o si tiene posibilidad de hacer compras de alto valor. Aunque no necesariamente a todos y todas nos molesta la publicidad, esta puede convertirse en intrusiva, o incluso puede influenciarnos de manera negativa.

Un delincuente puede buscar a través de los datos personales, saber, por ejemplo, cuántos hijos tiene alguien o dónde estudian, cuánto dinero tiene disponible en el banco, el estado de ánimo, entre otros. A través de estos puede planificar sus delitos de diversa índole: trata de personas, sextorsión, grooming y pornografía infantil, suplantación de identidad, comercialización de documentos falsos, entre otros. Un ejemplo de venta de documentos falsos se encuentra en este enlace y hacemos la recuperación de pantalla del precio del pasaporte, carnet de identidad y licencia de conducir bolivianos http://www.realdocproducers.com/Price_List.html

Uruguay	$2500	$700	$950
Bolivia	$2500	$700	$950
Afghanistan	$2500	$700	$950
China	$2500	$700	$950

Y una nota de la BBC *¿Sabe usted cuánto cobra el crimen organizado por un pasaporte falso?*, muestra cómo la venta de pasaportes legales y falsos es un gran negocio entre refugiados por la guerra en Siria http://www.bbc.com/mundo/video_fotos/2015/10/151013_video_migrantes_venta_documentos_falsos_ig

Es por esto que en muchos países ha surgido el derecho a la "protección de datos personales", el cual está destinado a dar garantías a las personas que sus datos no serán usados para fines comerciales, que las empresas que los resguardan (como los bancos o Facebook), no los venderán a terceros o pondrán en manos de delincuentes, y que esta información no será usada en contra del usuario. Este uso de datos personales, viola directamente el derecho a la privacidad que tenemos las personas, por lo cual la protección de nuestros datos personales reviste gran importancia.

2.3. Legislación de protección de datos en Bolivia

En Bolivia nosotros no tenemos una norma específica sobre la protección de datos ni una entidad que se encargue de esta materia, mucho menos se consagra en la constitución, sin embargo, tenemos el habeas data administrativo y el habeas data constitucional llamado también acción de protección a la privacidad, empleamos un sistema mixto comprensivo de la tendencia del derecho a protección de datos Europea y del habeas data más de popular en los países de Latinoamérica.

En todo caso, la noción de la protección de datos personales está poco desarrollada, relatamos un caso que ejemplifica esta situación, el número de cédula de identidad es un dato personal de carácter público y discrecional o a solicitud, porque no está a disposición de libre acceso de cualquier individuo. El titular de ese número decide cuando exponerlo a terceros con diversas finalidades: transacciones bancarias o como mecanismo de identificación para ingresar a ciertas entidades o establecimientos, pero también puede ser requerido y registrado por la autoridad pública ante una situación migratoria o de investigación policial para cuyo efecto el ciudadano está en el deber de proporcionar su cédula e identificarse. Sin embargo, este número de identidad, albergado en bases de datos puede ser utilizado para obtener información como es el caso electoral para saber el recinto de votación (http://yoparticipo.oep.org.bo/aplicaciones/consulta), de tal manera que si una persona conoce tu número y tu fecha de nacimiento también podría saber el lugar de sufragio al cual acudirás, e inclusive si eres jurado electoral. El Órgano Electoral no ha previsto ningún tipo de regulación jurídica tal como condiciones de uso o políticas de privacidad, desde un doble ángulo este servicio electrónico puede ser utilizado como un perjuicio en manos de un caso de acoso o persecución con lo cual se crean riesgos para las personas pero también un beneficio de acceso a información pública, en todo caso podrían hacerlo mejor y proporcionar un nivel de seguridad más amplio quizás con algún tipo de validación adicional.

2.4. El negocio de la seguridad informática

Según un estudio de la empresa Kaspersky, las empresas grandes invierten hasta 1 millón de dólares en seguridad informática al año pesar que tienen dificultades en identificar el retorno de las inversiones en seguridad informática, “los negocios de cualquier tamaño concuerdan que continuarán invirtiendo en mejorar la seguridad informática independientemente del ROI, ya que es mejor pedir perdón que pedir permiso.” Este es un ejemplo de la forma en que el negocio de la seguridad informática se presenta, mostrando que los ataques son frecuentes y que las empresas deben invertir altas sumas para prevenir. De esa manera, es uno de los rubros con mayor crecimiento los últimos años.

Ya en 2012, PricewaterhouseCoopers (PwC) identificó que el negocio de la seguridad TIC generaba anualmente un volumen de negocio cercano a los 60.000 millones de dólares.

En el 2012, este boom que beneficiaba a las empresas de seguridad lograba que sus sus ganancias se incrementan de forma exponencial, incluso en empresas maduras como Symantec (14,1%) y por supuesto en las más jóvenes de las características de Fortinet o Sourcefire, que suben en torno al 51% anual.

Debido a que los datos son tan apreciados por delincuentes, empresas e incluso gobiernos vamos a ver a continuación algunos softwares maliciosos que se desarrollan con el fin de hacerse de los datos personales u otras formas de extorsión, tipos de ataques para afectar sitios web y bases de datos fraudes, y engaños comunes que vivimos a diario e intentan adueñarse de nuestros datos, delitos que se cometen utilizando esos datos y algunas prácticas empresariales que son criticadas con el objetivo de controlar y gestionar esos datos.

3. Softwares maliciosos y tipos de ataques

Existen básicamente dos tipos de ataques que pueden afectar a nuestras computadoras, dispositivos, información y páginas web. El malware y el ataque de denegación de servicio.

3.1. ¿Qué es un malware?

El malware es un programa maligno y malintencionado que tienen por objetivo dañar tu dispositivo y la información que tienes. Algunos tipos de malware según su intención son:

- **Malware para la creación de puertas traseras.** Es una modificación al sistema de modo que se creen entradas escondidas al mismo para que los crackers entren a la red todas las veces que requieran de manera indetectable. Es, literalmente, como crear una puerta a la casa de alguien sino que éste se entere.
- **Drive-by downloads (Fantasmas de computadora).** Son pequeños pedazos de código de programación que se descargan al ingresar a ciertas páginas web y se instalan en los dispositivos para robar información, o para otras funciones, que van desde afectar al funcionamiento del sistema hasta inutilizarlo.
- **Rootkits.** Modifican el sistema operativo para volverse invisibles y desde ahí tienen acceso al código fuente de cualquier programa y modificarlo. Este malware es usado incluso por grandes compañías para evitar que los dispositivos puedan ejecutar música o videos piratas o no autorizados por ellos.

3.2. ¿Qué es un virus?

Los virus son un tipo de malware más específico. Están diseñados para dañar la información o cambiar alguna de las funcionalidades del sistema que usas. Estos programas informáticos dañinos se instalan en tu sistema sin consentimiento o conocimiento por parte del usuario, pero se ejecutan con alguna de las acciones de estos (Cuando se abre el programa infectado, por ejemplo). Una vez instalado en el sistema, empieza a funcionar de la misma manera que un virus biológico que invade el cuerpo humano (de ahí su nombre), por lo que empezará a copiarse a sí mismo y a infectar otros programas, archivos y unidades de información. Normalmente, los virus causan los siguientes problemas:

- **Modificar funcionalidades del dispositivo o quitar algunas.** Los virus pueden alterar como funciona tu computadora o celular, haciendo que se gaste más batería, el dispositivo se sobrecaliente, no se pueda acceder a algunas funciones básicas, entre otras.
- **Destruir grandes conjuntos de información.** Eliminar definitivamente importantes archivos como registros contables de tu empresa, documentos, etc.
- **Bloquear redes informáticas afectando al tráfico.** Evitar que puedas conectarte a internet o acceder a ciertas páginas web, o hacer que tu computadora acceda a páginas sin tu consentimiento o acción tuya.
- **Molestias como aparición de pop-ups.** Pequeñas bromas y molestias al usuario, de modo que no puedas usar tu dispositivo con normalidad, haciendo que éste se reinicie constantemente, que te aparezcan anuncios masivos, entre otros.

No todos los virus son creados iguales y tienen los mismos objetivos. Aquí te presentamos una pequeña lista de los más conocidos tipos de virus en relación a cómo funcionan:

- **Los que se alojan en la memoria**. Obtienen el control de la memoria del dispositivo y así, pueden llegar afectar a todo archivo que se abre o ejecuta. Al tener control de la memoria, pueden canalizar mayor capacidad asimismo, afectando a que otros programas no tengan memoria y no puedan ejecutarse.
- **Virus de acción directa**. Estos virus sólo buscan replicarse varias veces ocupando mayor espacio. EL virus afecta uno tras otro cada archivo que encuentra. Cambian de ubicación constantemente.
- **Virus de sobreescritura**. Estos virus borran tu información o la inutilizan al reemplazarla. Es el más fácil de detectar pues el archivo infectado se modifica.
- **Virus de arranque**. Este inutiliza el arranque del sistema, afectando la usabilidad del dispositivo. Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco o unidad de almacenamiento CD, DVD, memorias USB, etc.
- **Virus polimórfico.** Estos cambian su código y se encriptan, de modo que ningún software antivirus puede detectarlo y encontrarlo.
- **Virus fat.** El más común en las memorias flash, es aquel que se instala sobre la unidad de almacenamiento e impide el acceso a ciertas secciones evitando que se pueda, al mismo tiempo, acceder a archivos importantes.
- **Virus de secuencias de comandos web.** Son aquellos que se ejecutan a partir de páginas web y generan acciones molestas como invasión de pop-ups, publicidad masiva o hasta porno.
- **Virus recycler.** Reemplaza el acceso directo a un programa y lo elimina o lo oculta.
- **Troyano.** Es un virus que ingresa al sistema desde otro programa mayor que lo carga y lo vuelve indetectable, como la historia del “caballo de troya”.
- **Bombas lógicas.** Son virus que se activan al cumplirse una acontecimiento determinado: por ejemplo fechas, combinación de teclas, condiciones técnicas.
- **Gusanos.** Se duplican a sí mismos hasta invadir todo el sistema.
- **Hoax.** No son propiamente virus, sólo información o contenido falso que los usuarios reenvían a sus contactos pensando que son cadenas de oración o campañas humanitarias

(ejemplo: reenvía este mail a 50 personas y Microsoft regalará 1 dólar por cada mail a un niño en Somalia). Su intención es simplemente llenar de tráfico innecesario la red.

3.3. ¿Qué es el Spyware?

Está creado para recopilar información del usuario y transmitirla a una entidad externa, sin el conocimiento y/o consentimiento del propietario de la información. Es decir, es un programa espía.

Este programa malicioso se instala en el sistema de manera oculta y se ejecuta cada vez que arranca el sistema (cuando se lo enciende), consumiendo energía y capacidad en la memoria. Funciona todo el tiempo y control y registra todo lo que se hace con el dispositivo.

Las empresas lo utilizan para saber qué hacen los usuarios cuando navegan en internet, qué páginas visitan o qué intereses tienen. Los gobiernos lo usan en cambio para vigilar actividades sospechosas y detectar potenciales amenazas. Los grupos delincuenciales, para acceder a contraseñas secretas y datos de usuario y así entrar a cuentas bancarias o secuestrar correos electrónicos.

Algunos de los spyware más conocidos son:

- CWS. Se instala en el navegador de internet para conocer todo lo que visita el usuario e incluso redirigir sus búsquedas hacia páginas concretas.
- Gator. Es un programa que abre ventanas y anuncios de publicidad en base a las preferencias y gustos del usuario.
- Internet optimizer. Reemplaza ciertas páginas, sobre todo las de error, y las reemplazan por otras.
- N-CASE. Rastrea los hábitos del usuario para conocer sus preferencias y gustos.
- Transponder. Se instala sobre el navegador para guardar datos de formularios, contraseñas, etc.
- Perfect Keylogger. Guarda registros de contraseñas y registros de teclas usadas para dar con información confidencial.
- Pegasus. Es uno de los malwares más sofisticados que existe y tiene una capacidad de vigilancia total. Puede leer los mensajes y correos del usuario, escuchar llamadas, hacer capturas de pantalla, registrar claves que se introducen, acceder al historial del navegador, contactos, etc. Básicamente, puede espiar cualquier aspecto de la vida de la víctima. Ataca tanto dispositivos Android como Apple, con la diferencia que en el primero puede intentar múltiples formas de ingresar al sistema de la víctima mientras que en el segundo, si no lo consigue, simplemente se autodestruye.

3.4. ¿Cómo evitar ser atacado por virus, malware o spyware?

Aquí damos algunos consejos muy útiles para mantenerte lejos de estos bichos indeseables:

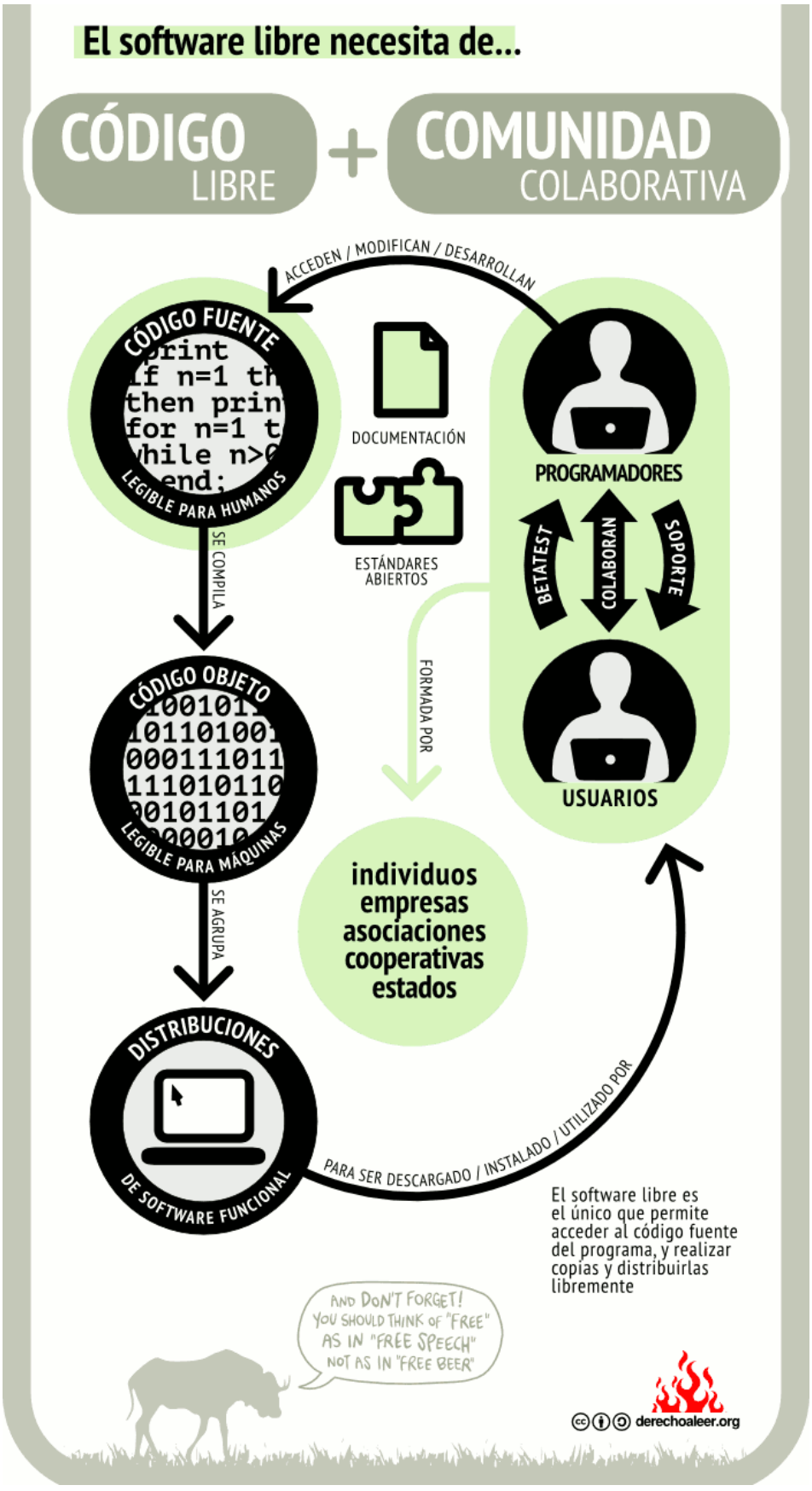
- Instalar un antivirus adecuado y actualizarlo de manera constante. No te quedes simplemente con el antivirus que viene por defecto en tu computadora. Hay software antivirus muy poderoso en el mercado a bajo costo, incluso gratuito, algunos de los más conocidos y usados son Avast, NOD32, Kaspersky, AVG.[1]
- Instala un software anti-spyware. Los antivirus no necesariamente te protegen contra el software espía. Normalmente, es mejor tener un software aparte. Algunos recomendados son: Spybot, search and destroy,[2] el cual es un programa veterano y muy fuerte, pero tiene un costo mínimo. Otro muy recomendale y gratis es: Malware bytes[3].
- Haz escaneos periódicos. Es importante escanear tu computadora o dispositivo regularmente, por lo menos una vez a la semana, o incluso diariamente.
- Evita ingresar a sitios sospechosos. Normalmente, los virus, se alojan en sitios pornográficos, de descargas gratuitas, películas u otros que pueden parecer atractivos.
- Desactiva la auto-ejecución de fotografías, archivos adjuntos o videos en tus correos, servicios de mensajería como whatsapp y otros servicios de redes. Al ejecutarse estos de manera automática, se ejecutan también los virus.
- No hagas click en anuncios de ningún tipo. Al darle clic, estás permitiendo que el software malicioso se descargue.
- Cuando instales algo, siempre fíjate de no aceptar que se instalen otros componentes como barras de buscadores, add-ons u otro peligro.
- Evita descargar aplicaciones, juegos y películas gratis y piratas. Normalmente, todo juego o aplicación gratuita que descargas contiene virus incrustado. Una manera de pagar por estos programas es justamente dejando que estos virus se instalen en tu computadora.
- Ten cuidado con los botones falsos de descarga. Cuando buscas descargar algo en páginas sospechosas, es posible que te aparezcan múltiples botones de descargar. Varios de ellos son para descargar virus y sólo uno es el real.
- Utiliza navegadores seguros y actualizados. Evita usar Internet Explorer o versiones antiguas de otros navegadores pues estos son más inseguros.
- Usar software libre ya que existen menos virus para este software y también que para ejecutar un archivo de virus pedirá la contraseña, lo que lo hace menos susceptible a contraer virus. Para conocer algunas características del software libre, a continuación un par de infografías.

[1] Link página de AVG para descargar antivirus gratuito https://www.avg.com/es-ww/free-antivirus-download

[2] Link: https://www.safer-networking.org/es

[3] Link para descargar: https://www.malwarebytes.com/mwb-download/


¿Qué es el Software Libre?
Es el software que garantiza la libertad de...
0 usar el programa con cualquier propósito
1 estudiar cómo funciona, modificarlo y adaptarlo a tus necesidades
2 distribuir copias del programa
3 mejorar el programa y publicar las mejoras
se debe poder acceder al código fuente
licencia libre
La licencia es el texto legal que garantiza que se cumplan las cuatro libertades del Software Libre.
Valores del Software Libre
solidaridad
activismo
ciencia
innovación
transparencia
robustez
no-discriminación
horizontalidad
libertad
estándares
meritocracia
compartir
política
eficiencia
bienes comunes
comunidad
hacking
colaboración
creatividad
educación
accesibilidad
ética
SOFTWARE LIBRE


El software libre necesita de...
CÓDIGO LIBRE
+
COMUNIDAD COLABORATIVA
ACCEDEN / MODIFICAN / DESARROLLAN
CÓDIGO FUENTE
print
if n=1 th
then prin
for n=1 t
while n>0
end;
LEGIBLE PARA HUMANOS
SE COMPILA
CÓDIGO OBJETO
100101
10110100
000111011
111010110
00101101
000010
LEGIBLE PARA MÁQUINAS
SE AGRUPA
DISTRIBUCIONES
DE SOFTWARE FUNCIONAL
DOCUMENTACIÓN
ESTÁNDARES ABIERTOS
FORMADA POR
PROGRAMADORES
BETATEST
COLABORAN
SOPORTE
USUARIOS
individuos
empresas
asociaciones
cooperativas
estados
PARA SER DESCARGADO / INSTALADO / UTILIZADO POR
El software libre es el único que permite acceder al código fuente del programa, y realizar copias y distribuirlas libremente
AND DON'T FORGET! YOU SHOULD THINK OF "FREE" AS IN "FREE SPEECH" NOT AS IN "FREE BEER"
derechoaleer.org

- Ignora alertas o mensajes de seguridad que no sean de tu propio antivirus. Normalmente, los crackers utilizan anuncios de seguridad para hacer exactamente lo contrario. Si te sale un anuncio así de una página cualquiera, mejor cierralo y haz un chequeo con tu propio software antivirus.
- Siempre escanea las unidades flash antes de ejecutarlas en tu computadora. Si alguien te da una unidad flash, por más que provenga de un familiar o amigo, haz un escaneo de virus.

¿Cómo hacer un análisis a tu computadora usando el antivirus Kaspersky? (Extraído de la página web del producto)

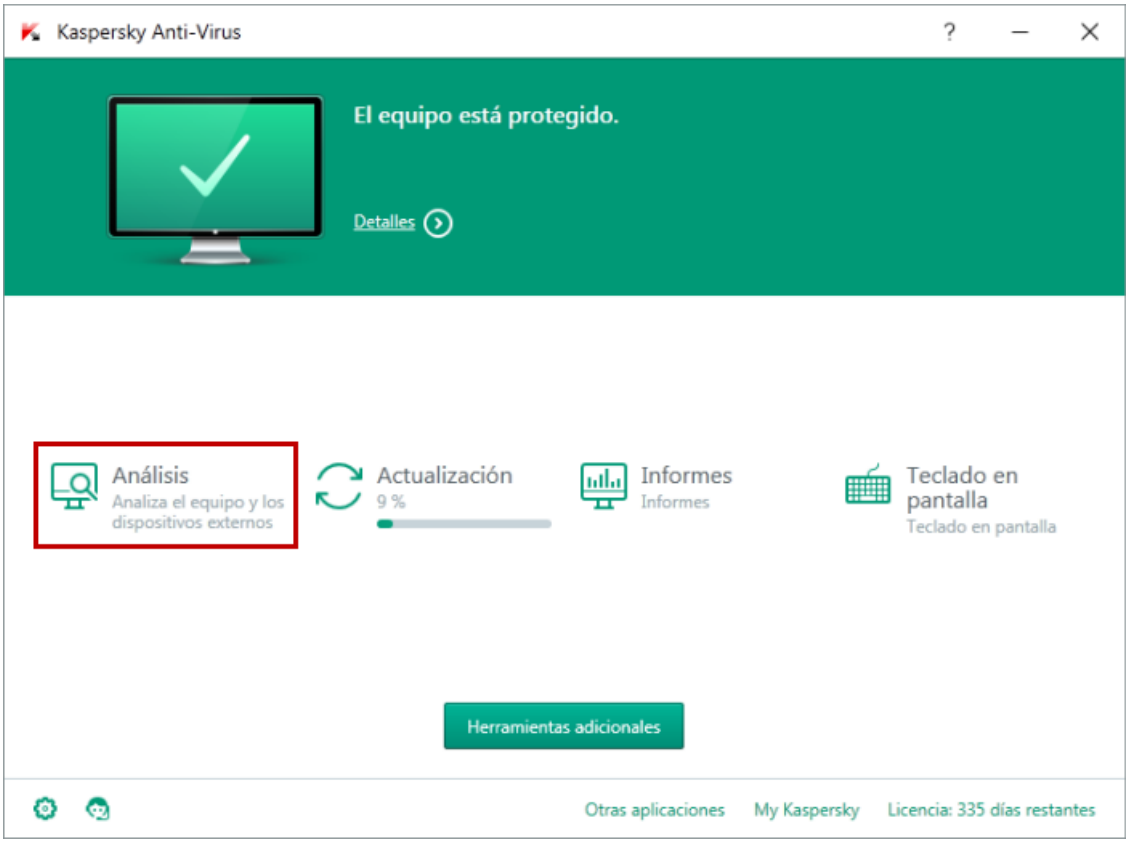
Análisis es un componente de antivirus importante destinado para detectar objetos maliciosos. Se debe realizar el análisis con regularidad para proteger el equipo frente a amenazas y software malicioso.

Los ingenieros de **Kaspersky Lab** han desarrollado los siguientes modos de análisis:

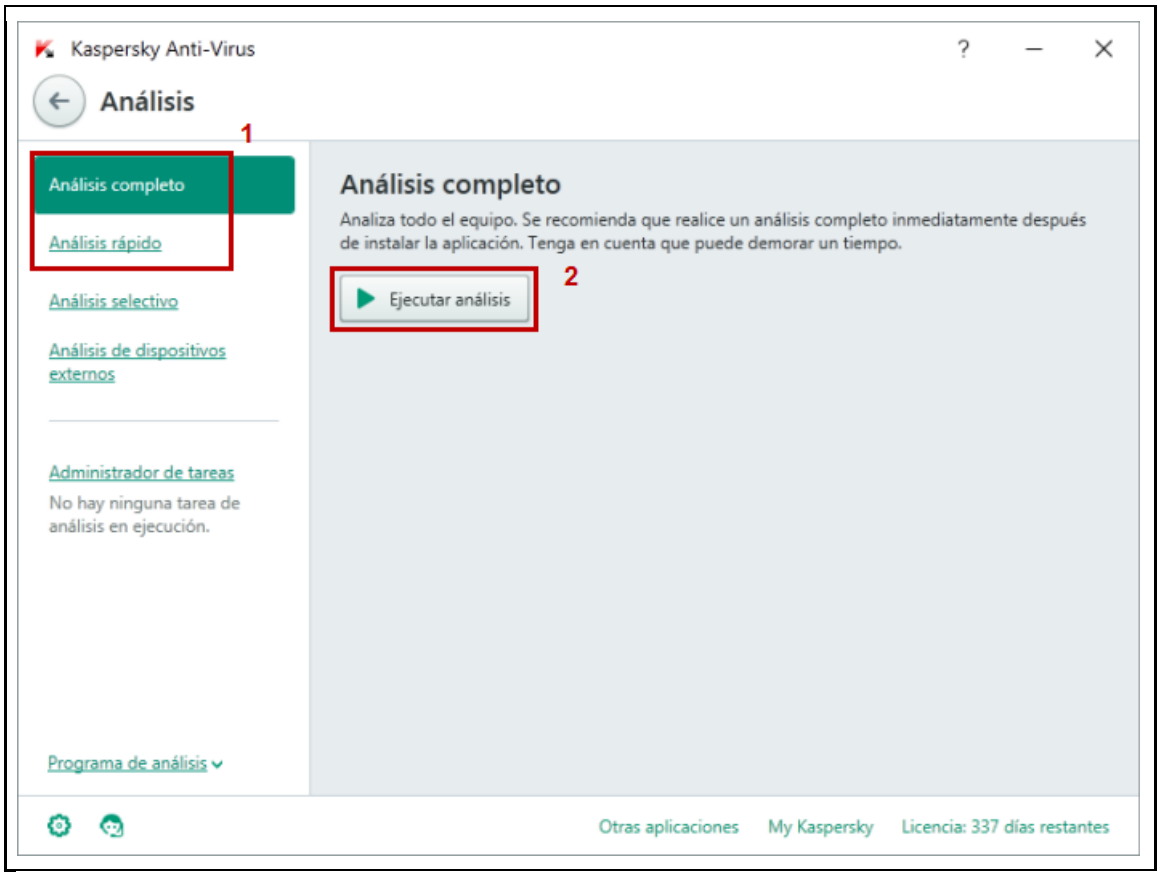
- **Análisis completo**: es el análisis de todo el sistema. De forma predeterminada, se analizan los siguientes objetos: memoria de sistema; objetos ejecutados durante el inicio; almacén de seguridad de sistema; bases de correo; discos duros y unidades extraíbles y de red.
- **Análisis rápido**: es el análisis de objetos que se ejecuten durante el inicio de sistema, así como el análisis de la memoria de sistema y bloques de arranque.
- **Análisis selectivo**: es el análisis de cualquier objeto del sistema de archivos.
- **Análisis de dispositivos externos**: es el análisis de las unidades extraíbles que están conectados al equipo.

Para ejecutar el análisis, realice lo siguiente:

1. Abra **Kaspersky Anti-Virus 2017**
2. Haga clic en **Análisis**.



1. En la ventana de **Análisis**, haga clic en **Análisis completo** o **Análisis rápido**.
2. En la parte derecha de la ventana, haga clic en **Ejecutar análisis**.



3.5. ¡La página se cayó! ¿Qué sucedió?

A menudo escuchamos que las páginas web se caen o que no se puede acceder a ellas. Esto puede ocurrir por varias razones, por ejemplo, que los encargados no pagaron el alquiler del espacio para alojar la página web (hosting). A veces también, puede tratarse de un ataque informático. Este tipo de ataques se llaman de “Denegación de servicio” o DDoS. Son ataques que hacen colapsar la capacidad de las páginas de atender visitas por parte de usuarios y dejan de funcionar.

Más técnicamente hablando, estos ataques se generan debido a la saturación de puertos con múltiples flujos de información, de modo que el servidor que aloja la página se sobrecarga y no puede atender más solicitudes de usuarios. Entonces, se cuelga y detiene su funcionamiento y hasta se apaga. Entonces requerirá que el servidor vuelva arrancar, el ataque se detenga o que se bloqueen las conexiones hasta reestablecer las capacidades del servidor. Para lograr eso, los atacantes se ponen de acuerdo para intentar ingresar de manera masiva a una página web hasta hacerla colapsar. También existen programas para automatizar estos requerimientos de ingreso masivos o formas de manipular las conexiones de otras personas u objetos y dirigirlas hacia el servidor que se va a atacar, por lo que cualquier persona puede estar siendo usada para hacer un ataque DDoS sin darse cuenta. Por ejemplo, el ataque de DDoS contra uno de Dyn, uno de los proveedores de

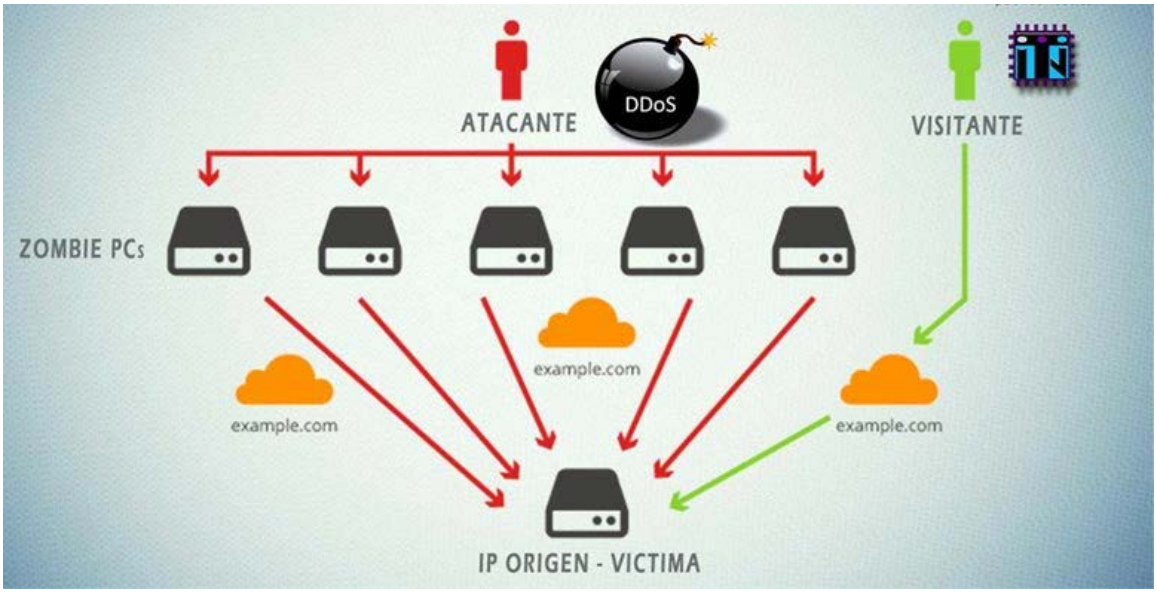
DNS más grande del mundo que dejó sin Internet a gran parte de la costa Este de EE.UU. durante un día durante el 2016. Lea este enlace para mayor información http://bit.ly/DDoScontraDyn

No todos los ataques DDoS son malos, pues a veces pueden estar dirigidos hacia páginas web maliciosas o delictivas, como por ejemplo, aquellas que pueden tener contenidos sensibles (racistas, pedófilos, entre otros).

En estos casos, todos deben cuidarse de posibles ataques DDoS porque pueden estar siendo usados para tales fines.

Para protegerse contra estos ataques, los dueños de los servidores que alojan las páginas web deben instalar filtros que puedan detectar IPs falsas y paquetes de información muy pesados, aunque estos no son infalibles. Hay buenos servicios como Kona Site Defender o AKAMAI que analizan y absorben el tráfico y lo redistribuyen a otros servidores, evitando que así estos colapsen. Este tipo de protección es sobre todo importante para empresas que hacen comercio electrónico, bancos u otras que dan servicio directo a la población y que no pueden estar fuera de línea ni por un momento.

Los usuarios deben cuidarse del malware o del spyware, pues es a través de estos que sus conexiones son mal utilizadas por terceros. Para evitar esto un usuario común debe cambiar las contraseñas que viene por defecto en los equipos que se conectan por wifi como las impresoras. Es decir, las contraseñas suelen ser “admin” o “123456” que deben ser cambiadas por alfanuméricas y por palabras que no estén relacionadas entre sí.



3.6. El hacking ético

El ciberespacio reproduce todos los aspectos positivos y negativos del mundo analógico, el mundo físico. En ese sentido, el ciberespacio es un mundo que nos ofrece muchas potencialidades: acceso a la información, posibilidad de entablar interacciones con personas de todo el mundo, encontrar trabajo, compra y venta de bienes y servicios, entre otros tantos; pero a la vez, es un mundo oscuro, en el cual existen peligros, se llevan a cabo delitos y estamos en riesgo.

3.6.1. Diferenciando hackers y crackers

Siendo así, en el ciberespacio encontramos personas o usuarios buenos y malos, héroes y villanos. Los héroes son los hackers – quienes a veces erróneamente son tildados como malos- y los villanos son los crackers. Sin embargo, la determinación de quiénes son hackers y quiénes crackers no siempre es fácil, por eso, muchas veces se hablan de hackers de sombrero negro, blanco o gris para determinar si sus acciones hacen daño o son beneficiosas.

A continuación te explicamos sus diferencias:

Hackers	**Crackers**
Los hackers son personas con grandes habilidades tecnológicas/informáticas que pueden alterar programas, acceder a dispositivos, incluir nuevas funciones en éstos, entre varios otros aspectos. Su motivación es cumplir desafíos y probarse ellos mismos, y al resto de las personas, sus capacidades para ingresar a los sistemas. Es decir, se guían por el mérito y la popularidad que obtendrán. No obstante, una vez realizan sus actividades de penetración de sistemas las reportan para que estas sean subsanadas. Son los que crean anti-virus, software libre y herramientas que pueden beneficiar a otros.	Los crackers son expertos en romper sistemas de seguridad e ingresar a sistemas sin autorización. Al igual que los hackers, poseen grandes conocimientos y habilidades informáticas. Su motivación es no sólo demostrar sus capacidades, sino sacar réditos de éstas a través de la extracción de información, extorsión o modificación de los sistemas para fines propios o de otros que los contratan. Incluso pueden simplemente crear el caos. Son los que crean los virus, malwares, spywares y otros males.

3.6.2. La ética hacker y el hacking ético.

Los hackers poseen una propia ética y código que es compartido por toda la comunidad de hackers a nivel mundial. Son valores y principios de los hackers:

· **La meritocracia.** Siguen y respetan aquellos y aquellas que han logrado demostrar sus capacidades, desarrollar software o herramientas que sirvan a otros.

· **La cultura abierta.** Creen que el conocimiento no es propiedad de nadie por lo que debe ser abierto para que todos lo aprovechen. Por eso han creado plataformas como Github, Wikipedia, Stackoverflow y otras en las cuales cualquier persona puede acceder a la información y beneficiarse de ella.

· **La colaboración.** Saben que las capacidades se fortalecen y los problemas se resuelven mejor cuando pides ayuda y dejas que otras personas te ayuden. Así, trabajan en comunidad, permitiendo que cada persona pueda contribuir de alguna manera. Este es el principio detrás de Wikipedia, por ejemplo, enciclopedia que ha sido desarrollada por millones de usuarios que cada día suben más artículos sólo con la motivación de compartir conocimiento.

· **El bien común.** Los hackers están altamente motivados por la idea de crear un mundo mejor. Por eso buscan hacer el bien a la humanidad, aportar de alguna manera con sus capacidades e ir en contra de aquello que perciben como malo o dañino para el resto. Es por eso que, por ejemplo, los hackers se han unido para boicotear a corporaciones, políticos o proyectos que puedan afectar a la sociedad.

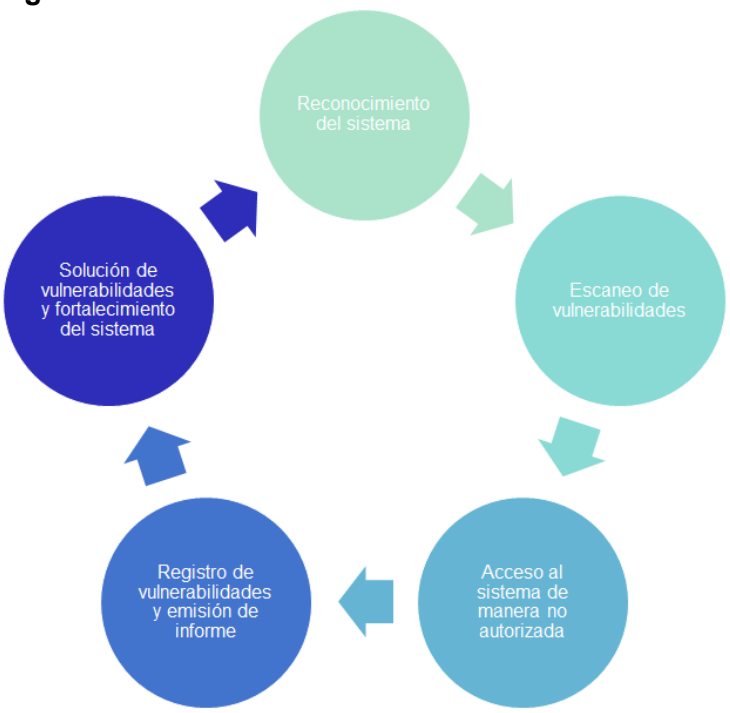
El hacking ético es el servicio de seguridad informática que ofrecen los hackers. Es una herramienta de prevención y detección de vulnerabilidades, a través de pruebas y ataques propios que intentan simular ataques de potenciales crackers y delincuentes. Se basa en los denominados “pen tests” o pruebas de penetración sistemáticas para encontrar errores y malas configuraciones.

Las empresas contratan a menudo este servicio en calidad de consultorías y auditorías informáticas para poder prepararse ante eventuales ataques de crackers. Es como realizar simulacros ante potenciales desastres. Si se va a necesitar el servicio del hacking ético, se sugiere contratar a empresas que sean certificadas por entidades u organizaciones, o personas que sean recomendadas y que tengan el aval de clientes anteriores.

El **hacking ético** debe de estar respaldado por lineamientos mínimos que deben ser parte de los contratos cuando se adquiere el servicio:

- Los hackers deben dar reportes completos de sus pruebas.
- Estos deben respetar el secreto industrial y la información a la que accedieron.
- Las auditorías deben hacerse bajo supervisión de los informáticos de la empresa.
- Se deben establecer límites claros con respecto a las actividades del consultor o consultora en seguridad informática.

Fases del hacking ético



Fases del hacking ético
1. Reconocimiento: Investigar toda la información posible que sea importante tanto para el cliente como para el potencial atacante. Esto va desde aspectos básicos como dirección IP, solicitudes de empleo, página web, etc. Si se identifica que es lo valioso y qué no, entonces se podrá hacer una mejor evaluación posterior. 2. Escaneo: el siguiente paso es identificar quienes son los usuarios y equipos que componen la red interna de la empresa. Se debe determinar qué puertos están conectados, cuales ejecutan servicios TCP (Protocolo de control de transmisión: El protocolo garantiza que los datos serán entregados en su destino sin errores y en el mismo orden en que se transmitieron), SSH (Intérprete de órdenes seguro-es el nombre de un protocolo y sirve para acceder servidores privados a través de una puerta trasera. Permite manejar por completo el servidor mediante un intérprete de comandos), entre otros, los cuales puedan facilitar la conexión al atacante. 3. Obtención de acceso: este paso es la ejecución de todas las maneras de ingresar a la red y al sistema de manera autorizada y no autorizada. 4. Generar informe de los incidentes que se hayan podido encontrar. 5. Solución de errores, vulnerabilidades, etc. Una vez se ha encontrado las vulnerabilidades del sistema, se deben solucionar los problemas y fortalecerlo. Esto ya no le toca al hacker, sino al ingeniero de sistemas o encargado tecnológico de la empresa o entidad, pero el hacker puede ayudar.

3.6.3. ¿Cómo beneficia el hacking ético a empresas y negocios?

El hacking ético es un servicio que ayuda a que las empresas, sin importar su tamaño, estén más seguras contra potenciales ataques. Las más atacadas, normalmente, son aquellas que pueden contener datos valiosos de sus clientes o información financiera. Es decir, sobre todo bancos, supermercados, empresas de comercio electrónico, clínicas, universidades y colegios, entre otras. En ese sentido, debería ser obligación de estas empresas brindar a sus clientes reportes periódicos del estado de su seguridad informática.

No obstante, justamente porque estas empresas están cada vez más preparadas ante potenciales ataques informáticos, los crackers cambian de estrategia con respecto al objetivo de sus ataques. Hay registros estadísticos que demuestran que los nuevos objetivos de los crackers son negocios pequeños y personas individuales, pues estos son los más desprotegidos y los que más subestiman la información que tienen. Desde los sistemas contables de un restaurant o un negocio mediano, hasta las fotos privadas de los usuarios, todas son vulnerables y valiosas, por lo que los crackers aprovechan para capturarlas y luego pedir recompensas.

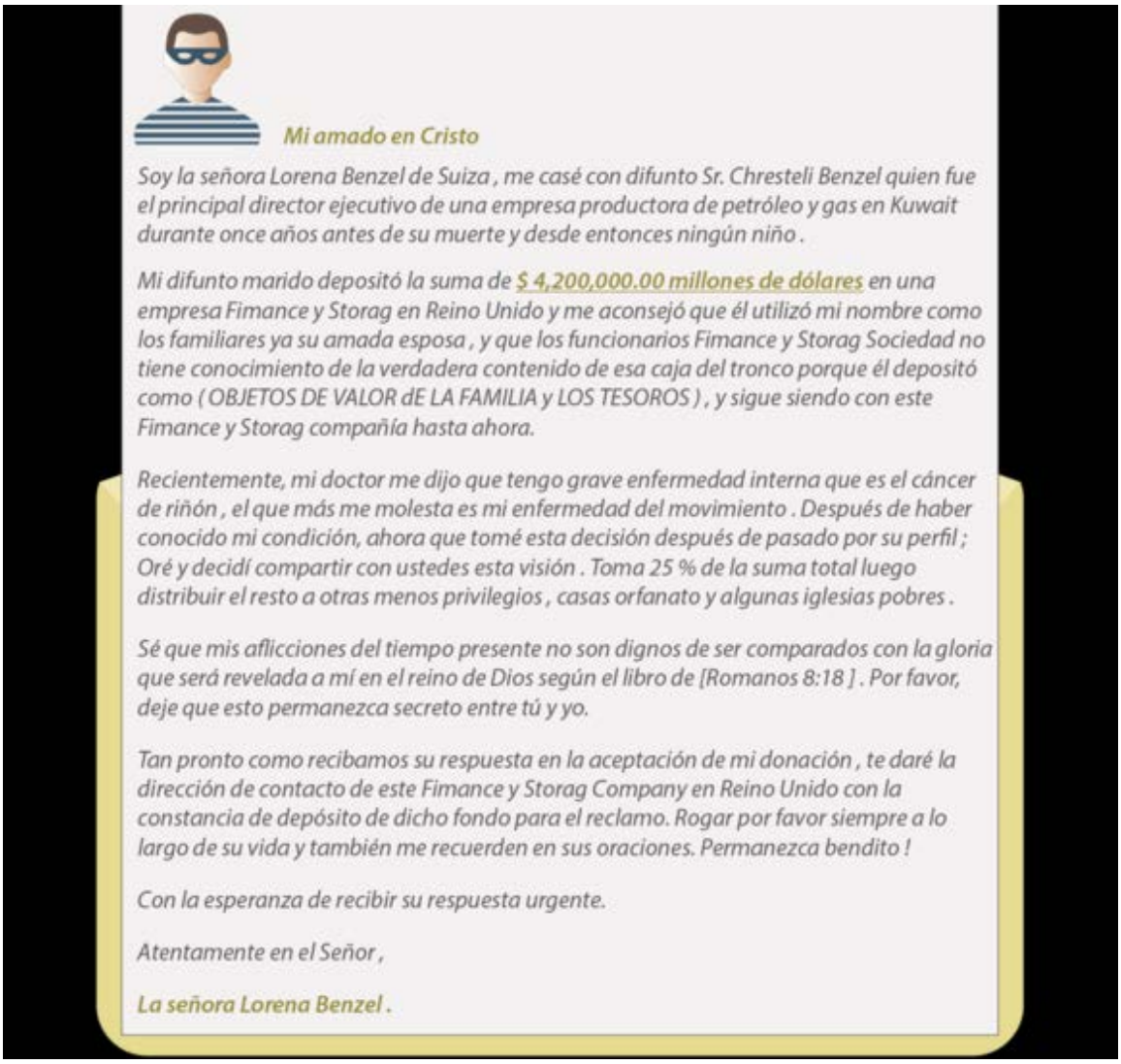
El caso más conocido, y el mayor ataque en la historia de la humanidad, fue el denominado ataque “WannaCry”, el cual afectó a más de 300.000 computadoras en más de 150 países, y sucedió a mediados de 2017. Esas computadoras eran sobre de todo de individuos comunes y empresas pequeñas.

4. Engaños y fraudes comunes

4.1. No, nadie te dará 5 millones de dólares en herencia por correo electrónico

Varias personas han recibido en sus correos electrónicos mensajes de amigos o parientes que dicen estar fuera del país y haber perdido todo el dinero y que requieren que se les envíe algún monto o mensajes de desconocidos explicando una situación en la que se requiere que depositen elevados montos en cuentas bancarias y piden que les pasen información de cuentas bancarias para hacerlo. Estas ofertas son tan buenas que parecen no ser ciertas. De hecho, no lo son, son crueles engaños.

Una de los engaños más usados a través de correos electrónicos es la famosa “carta herencia”, y es parecida a esta:



Mi amado en Cristo

Soy la señora Lorena Benzel de Suiza , me casé con difunto Sr. Chresteli Benzel quien fue el principal director ejecutivo de una empresa productora de petróleo y gas en Kuwait durante once años antes de su muerte y desde entonces ningún niño .

Mi difunto marido depositó la suma de $ 4,200,000.00 millones de dólares en una empresa Fimance y Storag en Reino Unido y me aconsejó que él utilizó mi nombre como los familiares ya su amada esposa , y que los funcionarios Fimance y Storag Sociedad no tiene conocimiento de la verdadera contenido de esa caja del tronco porque él depositó como (OBJETOS DE VALOR dE LA FAMILIA y LOS TESOROS) , y sigue siendo con este Fimance y Storag compañía hasta ahora.

Recientemente, mi doctor me dijo que tengo grave enfermedad interna que es el cáncer de riñón , el que más me molesta es mi enfermedad del movimiento . Después de haber conocido mi condición, ahora que tomé esta decisión después de pasado por su perfil ; Oré y decidí compartir con ustedes esta visión . Toma 25 % de la suma total luego distribuir el resto a otras menos privilegios , casas orfanato y algunas iglesias pobres .

Sé que mis aflicciones del tiempo presente no son dignos de ser comparados con la gloria que será revelada a mí en el reino de Dios según el libro de [Romanos 8:18] . Por favor, deje que esto permanezca secreto entre tú y yo.

Tan pronto como recibamos su respuesta en la aceptación de mi donación , te daré la dirección de contacto de este Fimance y Storag Company en Reino Unido con la constancia de depósito de dicho fondo para el reclamo. Rogar por favor siempre a lo largo de su vida y también me recuerden en sus oraciones. Permanezca bendito !

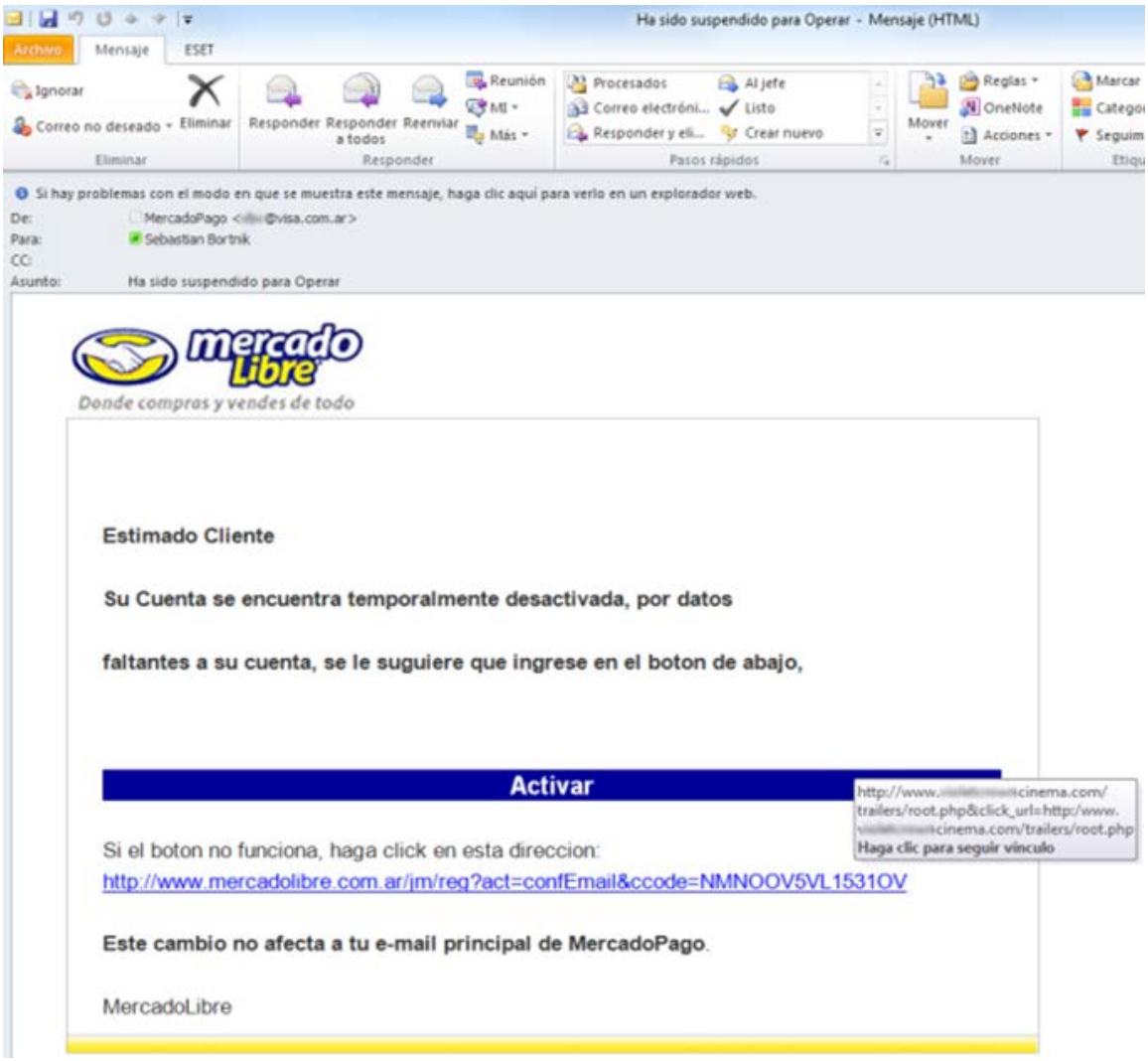
Con la esperanza de recibir su respuesta urgente.

Atentamente en el Señor ,

La señora Lorena Benzel .

El anterior correo muestra muchas señales de una posible estafa: la redacción es muy mala y poco clara, la historia difícil de creer y no explica cómo, de las 7 mil millones de personas que existen en el mundo, la Sra. Bezel justo dio con un correo de un ciudadano boliviano. Estas posibles estafas pueden contener las historias más extrañas e inverosímiles, desde herencias, oportunidades de negocio, dinero proveniente de alguien completamente desconocido, loterías en las cuales nunca se ha participado, hasta mensajes de celebridades. En realidad, son lavado de dinero.

Otro fraude muy común son los emails de compañías conocidas, sobre todo bancos, en los cuales se pide a la posible víctima que llené datos personales en un formulario ya sea para actualizar su información en el sistema o desbloquear su cuenta. La idea es que el usuario registre esa información y así, el delincuente la obtenga y pueda acceder a cuentas, hacer transacciones o compras. A este “modus operandi” se le conoce como *phishing* y tiene la intención de robar información secreta de la víctima para su uso ilícito.



A continuación te presentamos una lista de los tipos de engaño más comunes que se realizan por correo:

o Mensajes de bancos. Son correos provenientes de entidades financieras que piden que se actualice o provea alguna información con urgencia. No obstante, ningún banco te contactará por email pidiendo esa información. Normalmente tratará llamar o pedir que la persona acuda personalmente a sus oficinas.

o Cambio de claves. Son correos provenientes de alguna red social o servicio que se usa y que pide que se cambie la clave. Si no has requerido el cambio de clave tu mismo, es probable que este correo sea un engaño.

o Viajes o premios ganados. Te avisan que ganaste algo por lo cual nunca participaste. Los premios pueden llegar a ser tan atractivos que generen mucha tentación, pero sólo buscan que des información personal para redimir el premio. El problema es que nunca recibirás el premio

o Amigos extraviados en otros países. Pueden escribirte desde el propio correo de un amigo conocido pidiéndote ayuda. Es probable que tu amigo sólo haya caído en una estafa

de phishing y ahora estén usando su correo para hacer estafas más creíbles. Mejor intenta confirmar la información por otro canal o preguntale a otras personas para confirmar que efectivamente está de viaje y no es un engaño.

Los correos fraude tienen distintos elementos que los delatan:
- Apelan a la sensibilidad de las personas (un amigo perdido en algún lugar al cual nunca fue, el uso del dinero para beneficio de alguien con enfermedades terminales, etc.)
- Utilizan amenazas para ejercer coerción ("Si no mandas este mensaje, tu cuenta será cerrada", "Si no colocas tu información, congelaremos tu dinero por un mes", etc.)
- Piden información personal o de contraseñas y claves de seguridad al usuario.
- Tienen demasiados errores ortográficos y a veces poco sentido (las empresas grandes normalmente cuenta con editores profesionales que cuidan la buena redacción).
- Colocan enlaces (links) que no parecen lógicos con respecto a las páginas de las empresas de donde supuestamente provienen.
- Sus historias no son lógicas o son muy difíciles de explicar.
- No provienen de correos institucionales sino de correos genéricos (@gmail; @outlook.com; @yahoo.com, etc.)

4.2. ¿Cómo estafan por Facebook?

Facebook es quizás el espacio donde más fácilmente se pueden realizar estafas de todo tipo, esto pues a diferencia del correo electrónico, hay menos formas de filtrado de mensajes basuras (spam). A continuación, te presentamos algunas maneras para que las tomes en cuenta:

- **Solicitudes de amistad misteriosas.** Recibir solicitudes de amistad de personas completamente desconocidas no es normal. Hay que dudar, especialmente si no tienen amigos en común, o si resultan demasiado atractivas. Si aún así aceptaste a esta solicitud de amistad y la persona al otro lado te conversa y empieza a hacerte requerimientos, algunos de índole sexual, ten cuidado, puede ser que intenta adueñarse de material privado tuyo para después usarlo como manera para extorsionarte. La 'sextorsión' entre desconocidos (no confundir con la realizada entre personas que se conocen y exparejas, eso se llama pornovenganza) afecta al 3% de la población internauta. En Facebook, de hecho, se producen más de 54.000 casos al mes.

Aún si no se envía material sexual a ese contacto nuevo, puede extraer fotografías personales y modificarlas para intentar inculpar de algún crimen o usarlas para crear un perfil idéntico, invitar a los mismos amigos (quienes creerán que eres tú) y mandar mensajes a los mismos.

- **¿Quién ha visto mi perfil?.** Todos quisiéramos saber qué personas visitan nuestros perfiles y hasta con qué intenciones. Por ese motivo, los crackers han creado un malware que se aprovecha de ese deseo. En realidad Facebook no ha permitido aún esta funcionalidad, y cualquier oferta para instalar algún programa que te permita visibilizar esta

información es falsa. Lo que pasará es que darás click varias veces al enlace y jamás sabrás quién visitó tu perfil, sino que se descargará un programa malintencionado para extraer tu información personal.

- **Videos sexuales o raros.** Son varias las estafas que ofrecen mostrar videos pornográficos en Facebook, o videos bastante inusuales como un niño siendo comido por una boa. En realidad, estos videos son anzuelos para que se descargue software malicioso. Normalmente Facebook no permite la publicación de videos con contenido sexual, así que no hay que confiar. Lo peor de todo es que el software malicioso publicará en el muro de la persona que está haciendo clic en ese enlace malicioso para atraer a sus contactos y así, cada vez más gente cae.

- **Activar el botón "No me gusta".** No existe un botón oficial que pueda indicar exactamente lo contrario del famoso “like” o “me gusta”, sólo la cara de un emoticon que significa enojo. Cualquier oferta para instalar este botón es, sin lugar a dudas, un engaño.

- **Ofertas de productos.** Facebook se convirtió en una plataforma de compra y venta bastante útil y fácil de usar. No obstante, al igual que en cualquier otro medio, hay ofertas que pueden ser simplemente grandes engaños. Debido a su alta flexibilidad, con pocos mecanismos de comprobación de identidad, en Facebook abundan ofertas falsas que esperan pescar compradores incautos. Si buscas comprar algo por Facebook, asegúrate que el usuario sea legítimo, no des ninguna cantidad de dinero por adelantado ni datos personales de ninguna índole.

4.3. Identificando perfiles falsos

Las facilidades para crear cuentas y/o perfiles en distintas plataformas de redes sociales ha permitido la propagación de perfiles falsos que tienen diversas intenciones. Desde solamente ser cuentas para “trollear” o molestar a ser cuentas creadas específicamente para consumar hechos delictivos, estas cuentas falsas son abundantes y a veces difícil de distinguir. Para empresarios que desean hacer comercio electrónico, es importante lograr identificar estos perfiles para así saber si confiar o no en el contacto.

Aquí algunos consejos para evitar aceptar cuentas falsas:

- Fotos de perfil. Si la cuenta en cuestión solo tiene una foto de perfil una foto de perfil y unas pocas más, es muy probable que esta sea falsa.
- Actividad. Si la actividad de la cuenta es mínima o solo habla de un tema (publicita un producto, ofrece préstamos de dinero, hace campaña a favor o contra una organización política), esta podría ser falsa.
- Información general. Si el perfil no contiene información personal como lugar de estudio o trabajo, cumpleaños u otros, o es una persona muy precavida o posiblemente no es real.
- Google. Una forma rápida de descartar un perfil falso es buscando la foto de perfil en la web. Para ello solo hay que ingresar a la foto, hacer clic derecho y seleccionar "Buscar en

Google", en base a los resultados se podrá saber si se trata de una imagen real o una foto genérica.

- Una vez identificado un perfil falso, denúncialo usando las herramientas de Facebook.

4.4. Identificando noticias falsas

A partir de las elecciones presidenciales de Estados Unidos de Norteamérica en las que ganó Donald Trump y otros sucesos globales y nacionales de carácter político se han puesto más en vigencia la producción y difusión de noticias falsas. Estas noticias son creadas con diversos fines: generar mayor tráfico de visitas luego de atraer a usuarios a través del uso de titulares llamativos o sensacionalistas, influenciar a la opinión pública a favor en contra de alguna causa o persona, promover guerra sucia, entre otros objetivos. Las noticias falsas afectan a las tendencias y comportamientos sociales por lo que es importante tomarlas en cuenta pues las personas pueden reaccionar masivamente y generar fenómenos no deseados. Aquí algunos tipos de estas noticias:

- **Duda de los títulos:** De acuerdo con la red social, este tipo de contenidos suelen tener títulos llamativos escritos en mayúsculas y con signos de exclamación. Ejm: INCREÍBLE!!! o NO LO VAMOS A PERMITIR!!!
- **Observa con atención el URL:** Una dirección falsa o que imita una original puede ser una señal evidente de contenido falso. Muchos sitios de noticias falsas realizan pequeños cambios en las URL de las fuentes de noticias auténticas para imitarlas. Ejm: http: //lostiempos.com.bo/ por http://www.lostiempos.com/ ¿Cuál es el nombre correcto del sitio web del periódico Los Tiempos?
- **Investiga la fuente:** Asegúrate que la noticia esté escrita por una fuente de confianza. Si proviene de una organización desconocida, verifica la sección "información" para obtener más detalles.
- **Detecta si el formato es poco común:** Muchos sitios de noticias de este tipo contienen errores ortográficos o diseños extraños.
- **Presta atención a las fotos:** Las noticias falsas suelen contener imágenes o videos manipulados. En ocasiones, es posible que la foto sea auténtica, pero que la hayan sacado de contexto.
- **Comprueba las fechas:** El orden cronológico de las noticias falsas puede resultar ilógico, o incluso pueden estar alteradas las fechas de los eventos.
- **Verifica las pruebas:** Comprueba las fuentes del autor para confirmar que sean precisas. Si no se aportan pruebas o se confía en expertos cuya identidad no se menciona, es posible que la noticia sea falsa.
- **Consulta otros informes periodísticos.** Si ningún otro medio está reportando la noticia, es posible que sea falsa. Si aparece en varias fuentes de confianza, es más probable que sea verdadera.
- **¿La noticia es un engaño o una broma?** Facebook asegura que es difícil distinguir una noticia falsa de una publicación humorística o satírica, por lo que sugiere comprobar si la fuente de donde proviene suele realizar parodias, y si los detalles y el tono de la noticia sugieren que puede tratarse de una broma.
- **Algunas noticias son falsas de forma intencional.** Reflexiona acerca de las noticias que lees y comparte solo las que sabes que son creíbles.

5. Tipificación de delitos y marco legal

5.1. Cyberbullying y ciberacoso

5.1.1. ¿Qué es y qué no es el ciberbullying?

Esta práctica es el acoso psicológico constante entre pares, normalmente jóvenes, a través del uso de medios digitales: mensajería instantánea, redes sociales digitales, correo, foros, servicios de chat, videojuegos, etc. El ciberbullying no se da de un adulto a un menor o viceversa, siendo esas prácticas de otra índole, pero si se da cuando un adolescente atormenta, amenaza, humilla, acosa o molesta a otro.

El ciberbullying se da, en la mayoría de los casos, a partir de antecedes de hostigamiento en otros entornos en los cuales víctima y agresor pudieron haberse conocido: la escuela, el barrio, las canchas de fútbol, etc. El entorno virtual sirve como un espacio en el cual el bullying puede potenciarse debido a la anonimidad y la facilidad para ejercerlo.

5.1.2. ¿Cuáles son las características del ciberbullying?

- Anonimato: en internet es más fácil ocultar el anonimato del acosador o acosadores. El acosador también puede engañar a la víctima acerca de su identidad y hacerse pasar por otra persona. Es preciso tomar en cuenta que en la mayoría de las ocasiones, el acosador es cercano a la víctima.
- Repetición: el acoso se da de manera constante y repetitivas. Su intención es generar no sólo disgusto a la víctima, pero sobre todo agobio y mortificación.

5.1.3. ¿Por qué es especialmente grave el ciberbullying?

Es grave pues el agresor tiene aún más maneras de ejercer su práctica y la puede ejercer de manera aún más libre e incluso en anonimato. Ante el constante acoso y desprotección, la víctima puede optar incluso por el suicidio con tal de librarse del hostigamiento.

5.1.4. ¿Cómo se da el ciberbullying?

Las formas que adopta son muy variadas. Las herramientas y plataformas tecnológicas dan muchas posibilidades a los agresores y/o acosadores, y aún menos formas de control a la víctima. Algunas maneras que se pueden citar son las siguientes:

- Acoso con mensajes en todas las plataformas en las cuales la víctima tenga una cuenta. La víctima puede optar por bloquear al agresor, no obstante, siempre hay canales y formas de continuar con el acoso.
- Divulgación de imágenes comprometedoras de la víctima, varias de las cuales pueden tratarse de fotomontajes o memes burlones.
- Divulgación de chismes sobre la víctima entre todos sus contactos o datos sensibles.

- Crear perfiles falsos de la víctima con el afán de causar su enojo, o bien, subir fotos de la víctima en sitios web de concursos, o en los cuales se vota por las personas más feas, menos inteligentes, etc.
- Etiquetar a la víctima en conversaciones, fotos, videos u otros sin su consentimiento y sólo con el afán de causar su molestia.
- Subscribir a la víctima en sitios porno, revistas u otras que le puedan generar spam y problemas futuros.
- Dejar mensajes anónimos para la víctima en distintos lugares.

5.1.5. ¿Qué pueden hacer las víctimas?

- Evitar contestar a provocaciones. El acoso se alimenta de la respuesta.
- Intentar cortar toda relación o forma de comunicación con los agresores.
- No facilitar ninguna información, fotografía o cosas que pueden ser usadas en contra de uno. Esto, en especial, en redes sociales o por servicios de mensajería. Una vez que una foto se ha digitalizado es muy fácil que llegue a manos incorrectas.
- Guardar las pruebas del acoso.
- Si el acoso es continuo, discutirlo con alguien cercano, sobre todo familiares, en el caso de adolescentes, conversar con los padres, tutores o una persona adulta.
- No olvidar que hay soluciones. Hay formas de hacer que el hostigamiento se detenga. Las salidas extremas no son las únicas.

5.1.6. ¿Qué legislación ampara a las víctimas del ciberbullying?

- Código niña, niño y adolescente (Ley 548).
  - Art. 147 establece la tipificación de tipos de violencia pasibles a sanciones.
  - Art. 150 insta a la protección de los niños niñas y adolescentes en el sistema educativo contra tipos de violencia.
  - Art. 151 establece la tipificación de tipos de violencia en el sistema educativo.
- Ley Contra la Violencia y Acoso Escolar del Concejo Municipal de Cochabamba.

5.2. Phishing y robo de identidad

5.2.1. ¿Qué es?

Este término se refiere a un método utilizado por delincuentes para obtener información confidencial de un usuario y así suplantarlo usando sus claves e información bancaria, entre otros.

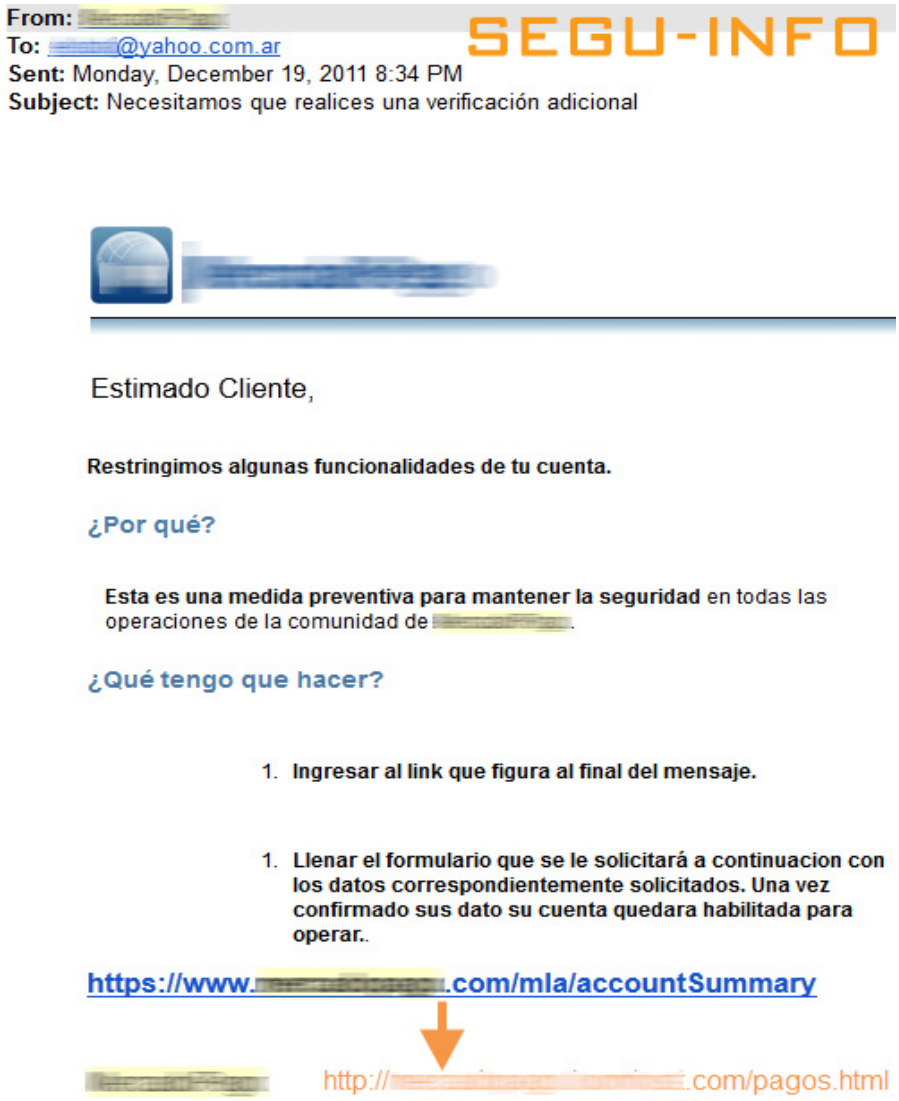
5.2.2. ¿Cómo se da?

El estafador utiliza distintas técnicas para extraer la información de la víctima. No es un hackeo o robo de información directo, sino que se trata de hacer caer a la víctima para que ésta sin darse cuenta proporcione su información. Normalmente, el estafador se hace

pasar por una persona o empresa de confianza de la víctima, usando por ejemplo un correo electrónico, un SMS, un mensaje en una red social, o incluso una llamada telefónica. Al tratarse una persona o empresa de confianza para la víctima, ésta proveerá la información que se le requiere y así el estafador podrá usarla para su propio beneficio.

- **Phishing por página web**

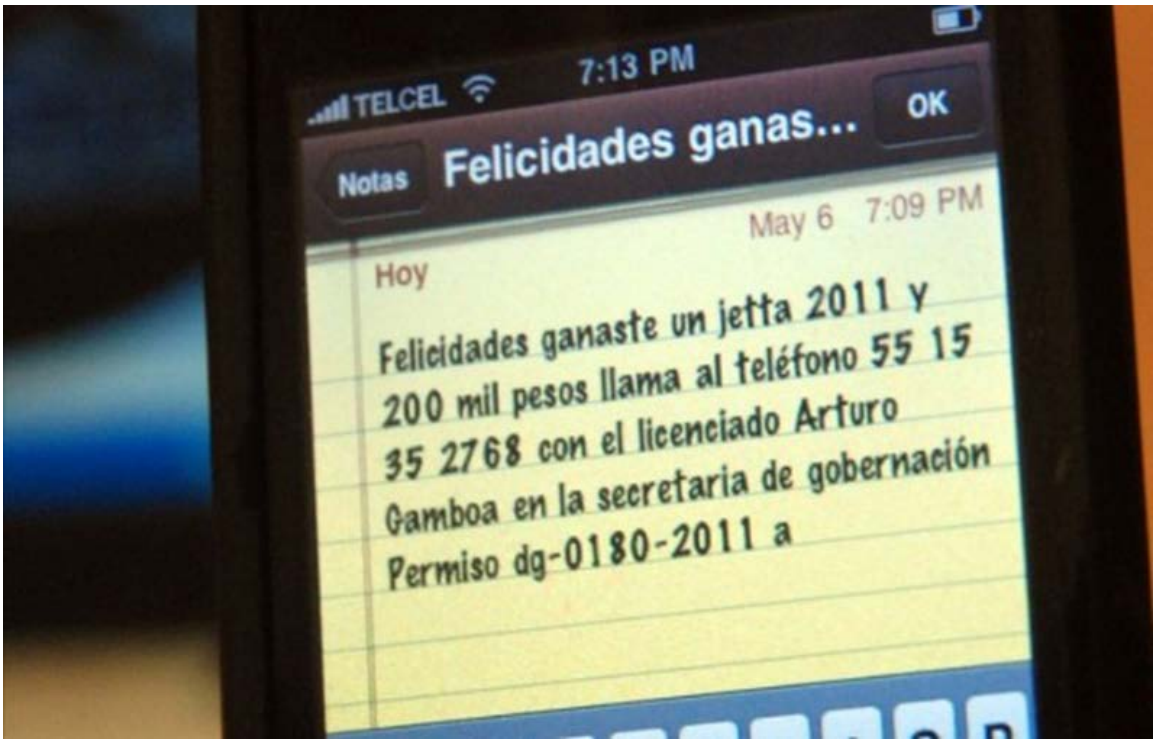
El estafador crea una página web idéntica al de una empresa o servicio, manda un correo a la víctima pidiendo que ésta coloque su clave para acceder a su cuenta, y una vez la víctima coloque su información, la página simplemente deja de funcionar. No obstante, la información se ha guardado y el estafador la ha guardado.



- **Phishing por SMS o mensaje**

El estafador enviará un mensaje alegando que la víctima ganó un premio y que para reclamarlo debe llamar un número o responder con alguna información: número de carnet de identidad, nombre de un banco o número de una cuenta para el depósito del dinero u

otra aún más sensible. De ahí el estafador, teniendo esta información previa, hará el phishing por página web o usará alguna otra técnica. Otra forma de hacer phishing de este tipo, es pidiendo a la víctima que compre una tarjeta de celular y pase el PIN al estafador.



- **Phishing por llamada telefónica**

El estafador llamará a la víctima y se hará pasar por un agente bancario, el proveedor de algún servicio o alguien relacionado a alguna empresa con la cual usted tiene alguna relación. Luego alegará algún problema grave por el cual debe ingresar a su cuenta con urgencia y requerirá se le facilite el PIN, clave o información sensible. Debido a la gravedad y preocupación de la víctima, ésta quizás provea la información.

5.2.3. ¿Cómo protegerse?

- Evite dar datos por correo electrónico, llamadas o mensajes, sobre todo si estos pueden derivar a su cuenta bancaria.
- No haga clic en enlaces que le llegan por correo que parezcan sospechosos. Es mejor escribir la dirección uno mismo en la barra de navegación.
- Compruebe que la página que ingresó tiene este formato: https:// (el “s” implica que es una página certificada) y un pequeño candado cerrado al lado (eso significa que es una página segura).
- Si sospecha que fue víctima de phishing, cambie todas sus contraseñas inmediatamente.
- A las personas que manejan dinero dentro de su empresa, hágales saber sobre los peligros del phishing y póngalas en alerta.

5.3. Ciberextorsión

5.3.1. ¿Qué es?

La extorsión es un delito que consiste en la intimidación o amenaza grave para obligar a una persona a hacer, tolerar que se haga o dejar de hacer alguna cosa, con el fin de obtener para sí o un tercero indebida ventaja o beneficio económico (Art. 333/Código Penal).

5.3.2. ¿Cómo se da en las redes sociales?

- **Obtención de información personal.** Se obtiene información personal de la víctima y se la usa para presionarla (datos, videos, fotos).
- **Uso de violencia o intimidación.** El o la extorsionador/ra utiliza mensajes, llamadas o cualquier tipo de contacto para localizar constantemente a la víctima.
- **La víctima es obligada a actuar de forma deseada por el extorsionador.** La víctima se ve obligada a realizar acciones que no son de su agrado para evitar ser agredida o evitar agresión a otras personas.

5.3.3. Tipos de extorsión en Internet

- **Sextorsión.** Se da cuando se amenaza de divulgar contenido sexual.
- **Grooming.** Un adulto desarrolla una relación con un/a menor para abusarle sexualmente.
- **Webcam.** Existe la amenaza de difundir contenido privado en video.
- **Secuestro virtual.** Se da cuando se pretende que hay una persona secuestrada pero en realidad no lo está y la víctima se obliga a hacer algo contra la voluntad si no quiere que le hagan daño al supuesto secuestrado.
- **Ransomware.** Virus informático que bloquea el acceso a la información que tiene una persona en su propia computadora y los atacantes piden dinero para devolverle el acceso.

5.3.4. ¿Cuál es la pena en la legislación?

De acuerdo al Código Penal, los delitos privativos de libertad (Art. 27) pueden tener penas desde 1 a 30 años. No obstante, la duración de la pena se puede ver modificada por el juez tomando en cuenta circunstancias como la edad, las costumbres, la conducta precedente y otros establecidos en el artículo 38.

5.3.5. ¿Qué hacer para prevenir y actuar frente a un caso de extorsión?

- No compartir información privada con perfiles sospechosos.
- No guardar fotos privadas en dispositivos de fácil acceso o de manera desprotegida.
- Tomar las fotos privadas evitando incluir el rostro y cualquier seña personal.
- Conservar la calma y no llegar a un acuerdo inmediato con el extorsionador.
- Intentar rastrear el servidor y el IP del agresor.
- Alertar a personas de confianza sobre la situación.
- Tener las *webcams* cubiertas si es que no están siendo usadas.
- No abrir *links* que puedan ser sospechosos.

5.4. Trata y tráfico de personas

5.4.1. ¿Qué es la trata de personas?

Son actos de coacción – actos violentos – a través de la captación, el transporte, traslado, aislamiento y/o recepción de personas, tratadas como mercancía. La coacción ejercida por una persona y un grupo de personas recurre a la amenaza, al uso de la fuerza, al engaño y al abuso de poder sobre personas en situación de vulnerabilidad, para comercializar sus cuerpos y vidas con fines de explotación. Las víctimas pueden ser trasladadas dentro o fuera del país, son privadas de su libertad para ser explotadas en distintas formas, las más recurrentes:

- Explotación laboral
- Explotación sexual (comercial)
- Matrimonio servil
- Empleo en actividades delictivas

IMPORTANTE: Cualquier persona puede caer en las redes de tratantes, no importa la edad o la condición económica. Los tratantes se aprovechan de la ingenuidad y necesidad de las personas.

5.4.2. ¿Cómo se da a través de internet?

Mientras se construyen prototipos de belleza y popularidad entre amigos, conocidos y amigos de los amigos en las redes sociales a través de la cantidad de *likes* y *followers,* las redes de trata y tráfico conocen esa lógica de interacción, se convierten en internautas y seleccionan sus víctimas a través de la información recabada en perfiles de Facebook, Instagram, twitter, etc.

Muchas veces los tratantes a través de perfiles falsos con fotos atractivas envían solicitudes de amistad a sus posibles víctimas, cuando son aceptados como amigos acceden de manera directa a toda la información de las personas (intereses, hobbies, disponibilidad a ciertas poses en fotografías) y además analizan las vulnerabilidades de las mismas a través de los estados que publican, de las descripciones que acompañan a sus fotografías, de las canciones y videos que comparten, etc. El siguiente paso es la intimidación, la cual puede darse a través de las mismas herramientas de las redes sociales y/o a través de salidas esporádicas. Al contar con suficiente información, muchas veces los tratantes acuden a las promesas sobre la base del *amor romántico*, en otras ocasiones en torno a los sueños de las mismas y otra veces se muestran como salidas al entorno fatídico de las víctimas.

Otras veces los tratantes conocen a sus víctimas en lugares físicos, en fiestas, conciertos, espacios de esparcimiento en general y posteriormente las agregan en las redes; de una u otra forma llegan al punto de escapar con las víctimas bajo el escudo del amor, o de viajar a escondidas para cumplir algún sueño, o simplemente tienen un cita en algún lugar no muy concurrido cuando aprovechan para raptar a las víctimas y tratarlas como mercancía.

5.4.3. ¿Cómo evitar ser otra víctima?

Los extorsionadores pueden ser personas conocidas o desconocidas, vivir en tu barrio ser amigos y hasta familiares; los mismos suelen acercarse a sus víctimas de forma amable o amistosa, te ofrecen invitaciones, regalos, dinero, viajes, mayores oportunidades de trabajo y mejor calidad de vida, inclusive se ofrecen a tramitar la documentación para poder salir fuera del país, por lo tanto puede ser complicado identificar si se trata de un tratante o un amigo (a) a conocer, entonces te sugerimos algunas acciones que pueden evitar que seas una víctima más:

- Limita el acceso a tu información sólo a las personas más cercanas a ti, no uses las redes para conocer gente ya que puede ser muy peligroso.
- Aléjate de personas que te aborden en la calle para conocerte.
- Si recibes mensajes en los que buscan seducirte, ilusionarte, amenazarte, chantajearte, intimidarte, o con la promesa de regalarte cosas que te gustan, conversa con una persona de confianza, de preferencia con tus padres o profesoras o profesores.
- Nunca hables con personas desconocidas en Internet y mucho menos actives tu webcam con ellas.
- Conserva los mensajes, correos electrónicos y toda información indebida, (como frases o imágenes ofensivas) servirán en caso de que sea necesario denunciar ante las autoridades.
- Nunca compartas información que sirva para identificarte o localizarte fuera de Internet, por ejemplo, los lugares que frecuentas, los días y la hora en que lo haces, los horarios en que estás en tu casa o los momentos en que te quedas a solas.
- Evita compartir tus estados de ánimo, ésta puede ser una herramienta eficaz para cualquier persona que quiera hacerte daño.

5.5. Esas personas que te acosan todo el tiempo se llaman trolls

Los trolls son personas que publican mensajes provocadores, irrelevantes o molestos en los foros, chats, comentarios en redes sociales, o en las páginas de algunas personas, empresas o entidades, con el único fin de molestar y generar emociones negativas. Suelen ser anónimos pero también pueden ser perfiles reales y que tienen relación con la organización o persona. Normalmente los motiva la diversión, pero a veces pueden llegar a la fijación con personas específicas; en el área comercial, los trolls también pueden ser competidores disfrazados que buscan el fracaso de su emprendimiento.

5.5.1. ¿Cómo identificar un troll?

Normalmente los trolls tienen este tipo de prácticas:

- Insultar. Los trolls insultan o llaman despectivamente a ciertos usuarios sin ningún motivo aparente.
- Discutir. Algunos trolls buscan polemizar o debatir por cualquier publicación de un usuario con la motivación de mostrar superioridad, molestar a la otra persona o hacerle perder el tiempo.
- Correcciones. Hay varios trolls que están a la pesca de errores ortográficos o de datos o fechas específicas de las publicaciones de las personas y buscan señalarlos de la manera más pública posible.
- Burlarse. Son trolls que minimizan o se burlan de las publicaciones ajenas para desviar la atención.
- Generar basura. Son trolls que buscan comentar a toda publicación posible con el fin de generar spam o basura, o incluso colocar links con el fin de arruinar la publicación de la persona.

5.5.2. ¿Cuál es el problema con los trolls?

Si no son controlados, los trolls pueden empezar a generar fijación con ciertas personas hasta convertirse en sus acosadores constantes y cometer delitos graves.

5.5.3. ¿Qué hacer?

- **Identifica al Troll**. Es necesario saber quién es un troll y separarlo de aquellos que quizás simplemente hicieron un comentario fuera de lugar. Si se sospecha que es un posible competidor, detectarlo a tiempo para evitar caer en su juego.
- **Trata de ponerte en contacto con el Troll**: Trata de establecer contacto privado para dialogar y hacerle saber que si continua con esa actitud, será bloqueado definitivamente. Es posible que el troll se trate de un cliente insatisfecho y será bueno saber el motivo de su insatisfacción.
- **No alimentes al Troll**. Si se le da más importancia de la necesaria, los trolls seguirán molestando. Al contrario, si son ignorados, desaparecerán.

6. Términos y condiciones de uso de los servicios más comunes

Las empresas de servicios de Internet suelen cobrar los costos con la captura de datos personales y uso de los mismos para marketing o incluso para cederlos a terceros, sean otras empresas o gobiernos. El valor de los datos hace que Facebook y Google sean de las más grandes a nivel global. Es importante, por tanto, conocer partes de sus Términos de usos que todos firmamos al abrir una cuenta en esos servicios.

6.1. Facebook

Es aconsejable leer las políticas de uso de Facebook así como su política de uso de datos. Aquí presentamos un resumen de ellas:

- El usuario o usuaria es propietario de todo el contenido e información que publica en Facebook y puede controlar cómo se comparte a través de las configuraciones de privacidad. Sin embargo, Facebook recopila toda la información de sus usuarios y usuarias, tanto la que proporciona, como la que otros usuarios y usuarias proporcionan de él, los métodos de pago, toda la información que proporcionen los dispositivos, los sitios web y aplicaciones que se usan para conectarse a Facebook. También recopila información que proporcionan los socios y empresas de Facebook como Whatsapp.
- Facebook no es responsable del contenido que los usuarios y usuarias compartan, tampoco de la conducta de los usuarios y usuarias dentro o fuera de Facebook.

- Se usa la información para personalizar lo mejor posible la experiencia del usuario/usuaria dentro de sus servicios, para comunicación, mostrar y medir la publicidad y servicios de sus anunciantes.
- Cuando se usa aplicaciones y sitios web de terceros, la información que se comparte con estas, está sujeto a sus propias condiciones y políticas.
- Facebook comparte información con socios y clientes, no se comparte información que identifique en forma personal al usuario o usuaria, es decir, Nombre o correo electrónico.
- En el caso de contenido protegido por derechos de propiedad intelectual, se concede una licencia no exclusiva, transferible, con derechos de sub-liciencia, libre de regalías y aplicable en todo el mundo a Facebook, esta licencia finaliza cuando se elimina la cuenta, salvo si este contenido fue compartido por otros usuarios y usuarias.
- Al publicar un contenido con la configuración “Público” significa que se permite que todos, incluso las personas que son ajenas a Facebook accedan, utilicen y asocien ese contenido a la persona que lo publicó a través de su nombre y foto de perfil.
- Se concede un permiso para que Facebook use el nombre, foto de perfil y todo tipo de contenido del usuario o usuaria. Es decir una empresa puede pagar a Facebook para mostrar el nombre, foto de perfil con el contenido e información sin que el usuario o usuaria reciba compensación alguna. Sin embargo Facebook respetará la configuración de Privacidad que se esté usando.

6.2. Whatsapp

- El usuario/usuaria acepta que las leyes, reglamentaciones y normas del país donde se almacena la información del usuario/usuaria, puede ser diferente de aquellas que rigen en su propio país.
- WhatsApp puede recopilar, usar, conservar y compartir la información del usuario o la usuaria si considera de buena fe que es necesario para procesos gubernamentales, exigir el cumplimiento de los Términos y Condiciones, detectar e investigar fraudes, proteger los derechos de los usuarios y usuarias, WhatsApp y la familia de empresas de Facebook.
- Si se comparte información con servicios de terceros como ser iCloud o Google Drive, se regirá bajo los términos y políticas de uso de esos servicios.
- En cuanto a la información que recopila de sus usuarios y usuarias, no conserva sus mensajes en sus servidores, los mensajes se almacenan en su propio dispositivo, en el caso de que un mensaje no se entregue de inmediato se conserva

por 30 días antes de ser eliminado. Pero si existe una foto y video muy compartido entre otros usuarios y usuarias, este puede estar más tiempo en los servidores.

- Recopila la información del dispositivo (modelo, sistema operativo, etc) y la información de su ubicación.
- Se usa cookies para mostrarle contenido relevante respecto de los servicios que brinda.
- Se le puede proporcionar mercadotecnia sobre los servicios de WhatsApp y los de la familia de empresas de Facebook. WhatsApp al ser parte de Facebook, recibe y comparte información con lo que llama familia de empresas de Facebook http://bit.ly/compañiasfacebook aunque hay controversias al respecto en la Unión Europea.

6.3. Twitter

- La empresa deja al usuario o usuaria como responsable de la publicación de información (texto o multimedia) que adquiere la categoría de pública que puede ser usada por terceros conectados a la red y por Twitter misma.
- Autoriza a recibir los servicios que ofrece Twitter, que están supeditados a las leyes de Irlanda, para el caso de Bolivia. Cuando se abre una cuenta a nombre de una institución, ésta también acepta esas condiciones.
- Privacidad. Al aceptar las condiciones el usuario o la usuaria acepta la aplicación de la jurisdicción legal de la empresa y da su consentimiento para la recopilación, almacenamiento y proceso de la información en Irlanda.
- Cuando los contenidos son publicados a través de la plataforma se da la licencia a Twitter y a terceros para el uso, copia, reproducción, procesamiento, adaptación, modificación, publicación, transmisión, exposición y distribución.
- La empresa también se reserva el derecho de borrar contenidos o eliminar o suspender cuentas de usuarios y usuarias que infringen las Reglas de Convivencia; o a hacer pública esa información en caso de que así lo requiera alguna petición legal aplicable en determinada región.
- Se prohíbe comportamiento abusivo como amenazas violentas, acoso, comportamientos que incitan al odio por raza, orientación sexual, etc., abrir cuentas en serie, publicación de información privada, suplantación de identidad, daños autoinflingidos, amenazas de suicidio, spam con malware o código malicioso.

6.4. Google y Youtube

Para tener una cuenta de YouTube es necesario tener una cuenta de Google, esto significa que los usuarios y usuarias también aceptan los términos y condiciones generales de Google que trascribimos a continuación:

- Todo el contenido que el usuario o la usuaria sube a los servicios de Google es suyo, al hacerlo el usuario o usuaria otorga una licencia mundial a Google para que use este contenido de diferentes formas con el objetivo de proporcionar, promocionar y mejorar los servicios y de desarrollar servicios nuevos, la licencia está vigente aún cuando el usuario o usuaria deje de usar algunos servicios de Google.
- El usuario o la usuaria puede dejar de usar los servicios de Google en cualquier momento, de la misma forma Google puede cancelar o eliminar un servicio por completo, notificando al usuario o usuaria antes de dicha situación para que extraiga sus datos de este servicio.
- Google no se hace responsable de la pérdida de beneficios, ingresos, datos, pérdidas financieras ni por daños indirectos, especiales, derivados, ejemplares o punitivos. En medida que la ley lo permita se limita al importe que se haya pagado por el servicio.
- Google no comparte información personal de sus usuarios y usuarias con empresas, organizaciones, ni particulares que no tengan relación con Google a menos que: el usuario o usuaria dé su consentimiento y los administradores de dominio en el caso de Google Apps, tratamiento externo empresas o personas afiliadas a Google.

7. Autodefensa digital

7.1. ¿Cómo cuidar tus datos?

Existen muchas prácticas ilegales por las cuales las empresas y grupos delictivos pueden obtener tus datos personales y sacar ventaja de ellos. Por ello, es preciso evitar lo siguiente:

- No permitas que crackers o empresas ingresen a tus correos o cuentas personales. Ten una contraseña segura, se cuidadoso de no dejar tu sesión abierta cuando utilizas una computadora ajena o en un Café Internet.
- No coloques tu teléfono en Facebook y de manera visible a todos. Borra este dato o colócalo en no-visible.
- No coloques tus datos en páginas que no sean de confianza tuya o hayan sido verificadas.

- Si es preciso, pide a las entidades bancarias o a las empresas a las cuales das datos personales que te muestren su política de protección de datos personales. Si no la tienen, demanda tu derecho a esa protección.
- Se consciente de tu derecho a la privacidad, tu información no tiene que ser pública si no quieres que lo sea.

7.2. ¿Qué hacer si te roban tu celular?

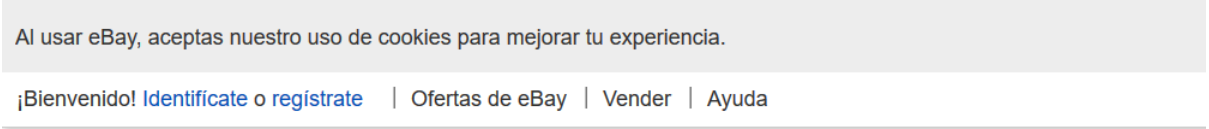
Tu celular es una de las mayores fuentes de información sobre ti que puede haber. Normalmente en tu celular se encuentra información sobre tus contactos (Agenda), las llamadas que realizas, los mensajes que envías, las fotografías que sacaste, los videos que viste, etc. Además, es el portal de acceso a tu cuenta de correo, a tus cuentas en redes sociales, e incluso, si tienes aplicaciones de bancos, a tus cuentas bancarias. Es decir, tu celular no es sólo un dispositivo caro, !es la llave a tu vida privada!

No obstante, nadie está protegido de su pérdida o robo. Por eso, debemos saber que acciones tomar si es que por alguna razón pierdes tu celular. Algunas acciones son:

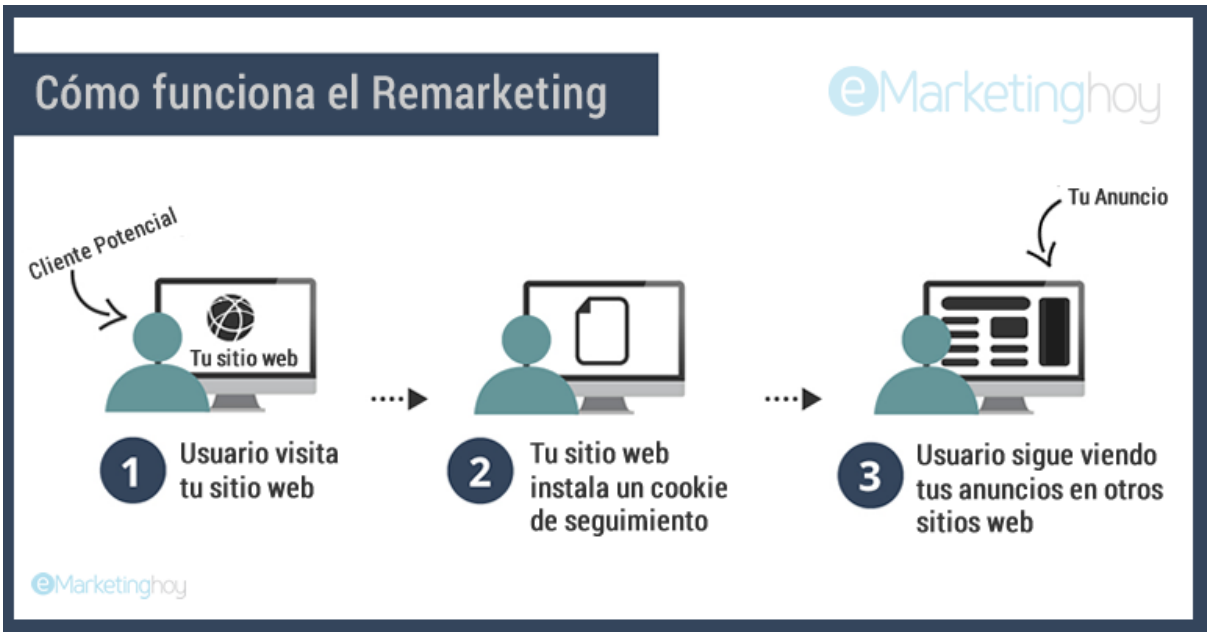
- Instala una app de control a distancia. Los celulares de última generación ya vienen con ésta pre-instalada, date el tiempo de configurarla y tenerla lista. Esta app te permitirá bloquear el celular si es que te lo roban o borrar toda la información.
- Ingresa a tus cuentas en redes sociales y correo, cierra sesión y cambia la contraseña inmediatamente.
- Avisa a tus contactos que tu celular fue extraviado, así que si reciben mensajes desde tu cuenta solicitando información, no la provean.
- Si tienes una aplicación o programa de un banco, llama al banco y pide que cancelen la autorización de tu teléfono para hacer movimientos bancarios.

7.3. Navegación segura y opciones libres al Google suite.

Nuestra navegación en internet genera continuamente datos que son guardados en distintos lugares, incluso en nuestras propias computadoras y dispositivos. Estos datos son como “migas de pan” que los usuarios vamos dejando en el camino y que pueden ayudar a que nos rastreen fácilmente y sigan nuestros pasos. Para obtener estas “migas de pan” las empresas tienen pequeños robots virtuales que se instalan de manera voluntaria en nuestras computadoras, estos robots se llaman “cookies” (galletas, en español). Siempre que entramos a una página web, automáticamente las cookies se descargan e instalan en nuestros dispositivos. Por norma, todas las páginas nos avisan que harán eso, por ejemplo, eBay, el famoso portal para hacer compras, te avisa que usará cookies.



No obstante, el problema es que no entendemos qué hacen las “cookies”.

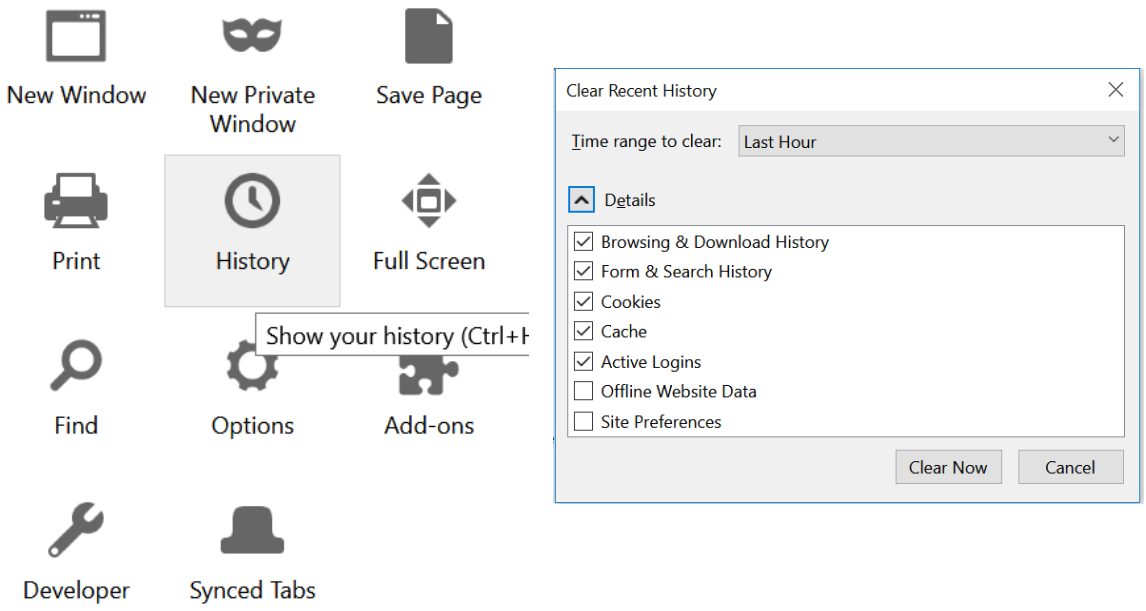


A través de las cookies y el registro de nuestras navegaciones, las empresas pueden colocar anuncios especializados y ofrecernos exactamente lo que buscamos. Eso en sí, aunque viola la privacidad, no es algo tan malo. El mayor problema es que, la navegación insegura puede permitir que delincuentes nos rastreen, los gobiernos nos vigilen y las empresas se aprovechen y jueguen con nuestra psicología.

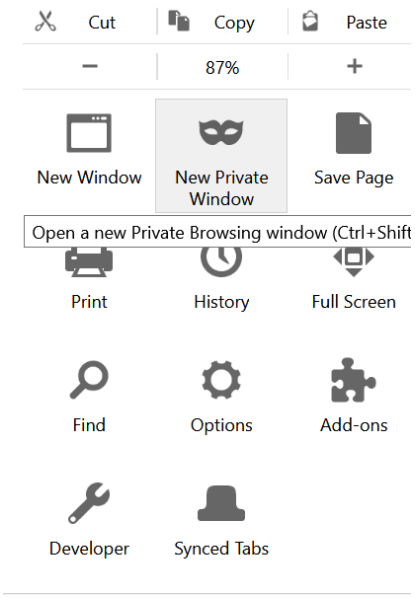
Un ejemplo muy claro es cuando intentamos comprar boletos de avión o reservar hoteles. Las empresas pueden, a través de nuestras cookies, saber que estamos buscando boletos para un determinado lugar, y aprovecharse de ello para anunciar que el destino al cual queremos ir tiene mucha demanda por lo que debemos comprarles sin importar el precio. Los usuarios entrarán en pánico y así lo harán, pero no se darán cuenta que en realidad las empresas saben de antemano que tenemos premura. Eso puede suceder con distintos productos.

Ese es sólo un ejemplo, quizás inofensivo, pero que demuestra los posibles usos que las empresas pueden hacer con respecto a nuestros datos de navegación. Los delincuentes pueden incluso encontrar mejores usos y saber así si tenemos disponibilidad de dinero, que estamos buscando viajar y probablemente nuestras casas quedaran desprotegidas durante nuestra ausencia, entre muchas otras cosas.

Por ende, se aconseja borrar las cookies de manera periódica. Esto es fácil de hacer si vamos a las opciones de nuestro navegador y borramos nuestros historiales de navegación.



Otra acción que podemos tomar, es navegar de manera segura. Puedes habilitar esta opción en tu propio navegador. Para ello, ve al menú desplegable de tu navegador y activa esta opción. Normalmente está referida como “navegación privada”, tal cual muestra la siguiente imagen.



Usando esta opción, tus acciones no serán registradas, no se descargarán las cookies y no quedará historial de lo que hagas. No obstante, esto no significa que estés protegido aún, simplemente no habrá registros de lo que hagas. El resto de las amenazas, siguen ahí.

Opciones de software libre a algunas funciones de servicios Google.

Será difícil utilizar en todos los casos software libre pero es bueno conocer algunas opciones libres que existen. Como ejemplo, las siguientes:

	Función suite Google	**Opción libre**
Correo electrónico	Gmail	Riseup, autistici
Almacenamiento	Gdrive	OwnCloud
Mapas	Google maps	Open Street Map
Navegador	Chrome	Firefox Mozilla
Calendario	Calendario	Sunbird
Traductor	Traductor	DeepL
Tienda de apps	Google Play	fDroid

7.4. Mensajería segura y encriptada ¿Es realmente necesaria?

A veces enviamos a través de nuestros correos información importante y sensible, desde contraseñas, fotografías, documentos importantes y otros.

En general no es aconsejable mandar información de este tipo por estos medios, pues pueden ser fácilmente accesibles por terceros a través de herramientas de monitoreo o crackeo de nuestras cuentas. Por otro lado, nuestra información siempre se transmite a través de los canales de las empresas de telecomunicaciones, es decir, estas empresas y el personal que trabaja en ellas podría fácilmente interceptar nuestra información y leerla. Finalmente, pueden hurtan nuestros dispositivos, dejamos nuestras sesiones abiertas en computadoras ajenas (en cafés internet o lugares públicos) y así leer nuestra información.

Si es que el usuario determina que es necesario generar mayores niveles de seguridad para sus correos y mensajería, presentamos algunas soluciones que se pueden intentar.

7.4.1. Encriptación, ¿Qué es?

La encriptación es el proceso para volver ilegible información sensible o muy importante. La información una vez encriptada sólo puede leerse aplicándose una clave que la descifra. Desde un aspecto técnico, la encriptación consiste en aplicar un algoritmo a nuestra información para convertirla en una cadena de letras, números y símbolos sin sentido. La encriptación no es algo nuevo, se practica hace más de 2.500 años.

Se trata de una medida de seguridad que es usada para almacenar o transferir información delicada que no debería ser accesible a terceros. Estas pueden ser contraseñas, números de tarjetas de crédito, conversaciones privadas, fotografías, etc.

7.4.2. Usa Signal en vez de Whatsapp

Signal y Whatsapp son herramientas buenas para la comunicación rápida y eficiente. Ambos son encriptados de punto a punto, es decir, en ambos los mensajes que salen desde el emisor van encriptados y seguros hasta llegar al receptor.

No obstante, hay una diferencia importante. Whatsapp guarda la metadata de los mensajes en sus servidores y Signal no. La metadata puede mostrar quién mandó el mensaje, desde dónde, a qué hora, usando qué dispositivo y número, entre algunos otros aspectos. La política de privacidad de Whatsapp menciona que incluso puede acceder a tus cookies, a los momentos en los que has estado conectado, a tu libreta de contactos, entre otros elementos privados de tu teléfono. Además, el dueño de Whatsapp es Facebook y combina las bases de datos personales de ambos servicios, es demasiada información personal en manos de una empresa. Esto combinación de bases de datos es ilegal en Europa pero no en el resto del mundo.

Signal, en cambio, no guarda ni accede a nada de esto, convirtiéndose en una opción mucho más segura si quieres proteger tu privacidad y evitar que te rastreen.

Al mismo tiempo, Whatsapp hace un back-up de tu información y la guarda en la nube (GoogleDrive o iCloud), por lo que si alguien accidentamente accede a tus cuentas de correo, puede automáticamente acceder a todas las conversaciones que tuviste con anterioridad.

7.5. Haciendo backup a la información importante, por si las moscas

Hay muchas razones por las cuales hacer un respaldo o backup a tu información. Puede que tu laptop o dispositivo sea robado, que tu disco duro falle por algún motivo, un virus del tipo “ransomware” y un cracker busque extorsionarte a cambio de devolverte tu información.

Para las empresas, tener un backup de su información puede ser la diferencia entre la vida o la muerte. ¿Qué pasaría si, por ejemplo, se borran todos los datos contables de la empresa? Se puede tener un backup en un dispositivo USB, disco externo,un NAS (Network-attached storage), o con almacenamiento en la nube.

7.6. Cuidando el hardware

Varios virus toman control sobre cámaras de computadoras y celulares, para evitar que eso dañe, lo más sencillo es tapar la cámara mientras no se la usa.

Bibliografía

Colectivo La Imilla Hacker. Taller de seguridad digital feminista. Cochabamba, julio 2017. https://aquelarresubversiva.net/theme/pdf/taller-manual-aquelarre.pdf

Derecho a leer. Infografía ¿Qué es el software libre? http://derechoaleer.org/blog/2014/04/que-es-el-software-libre-infografia.html

El Desarmador. Podcast. Programa Análisis de riesgos https://eldesarmador.org/07-analisis-de-riesgos.html

Kaspersky daily: Reporte: Midiendo el impacto financiero de la seguridad informática en los negocios https://latam.kaspersky.com/blog/reporte-midiendo-el-impacto-financiero-de-la-seguridad-informatica-en-los-negocios/7711/

6 DE NOVIEMBRE HASTA

9 DE DICIEMBRE
COCHABAMBA
BOLIVIA

Cursos **gratuitos**
para adquirir nuevo
CONOCIMIENTO
en el uso de herramientas
DIGITALES

Dirigido a emprendedores, pequeños empresarios
y población en general.

www.**internetbolivia**.org

Whatsapp
63192923

Facebook
/CursoInternetParaTodos

UNIVERSIDAD DEL VALLE BOLIVIA

UNIVERSIDAD UCATEC