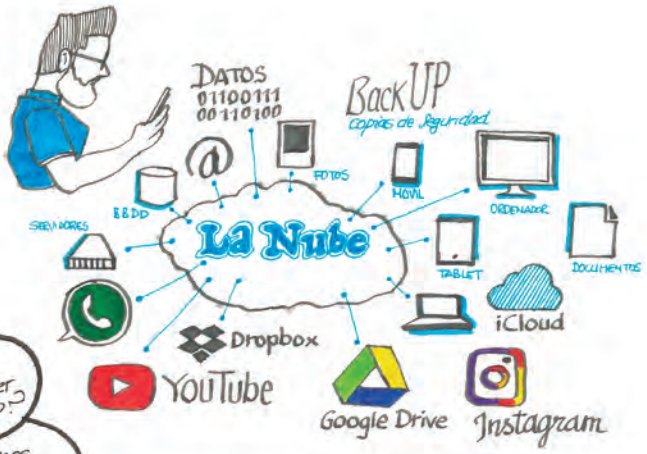
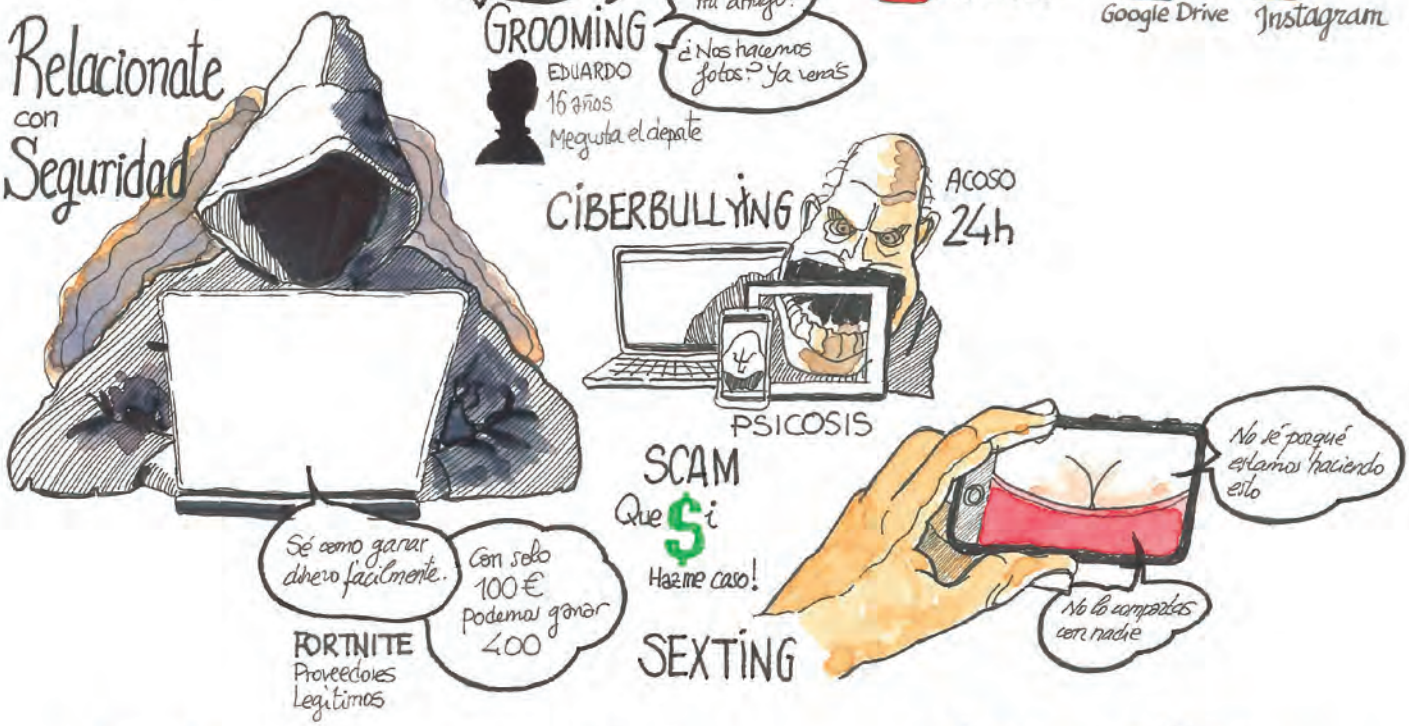
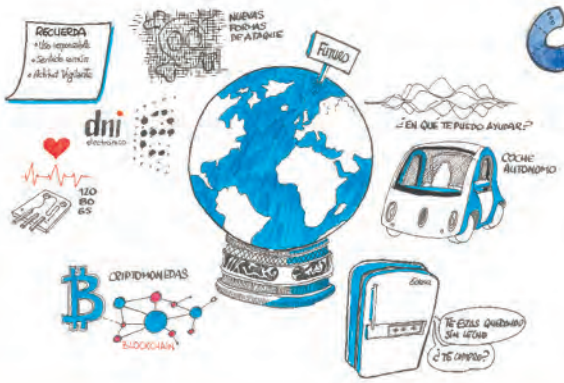
LA CARPETA







Número 172
monográfico
diciembre 2018

riesgos y amenazas en Internet RRSS

GOBIERNO DE ARAGON

El Instituto Aragonés de la Juventud como representante de todas las personas jóvenes que están en el territorio aragonés ofrece, a través de este documento, una herramienta que permita a todos los/as jóvenes, el profesorado, el alumnado, los/las tutores, los/as madres y padres y todas aquellas personas que están vinculadas a la juventud de una u otra forma, tener un recurso que les ayude para la detección y prevención de situaciones en riesgo que hay hoy en día en las redes.

La forma de comunicación varía de una forma vertiginosa a través de las diferentes redes sociales, formas digitales, foros, chats, juegos en línea, videojuegos, aplicaciones web,... con las que nos comunicamos diariamente con el mundo. Las personas estamos interconectadas de tal forma que nuestro objetivo no es sólo el de estudiar, aprender o informarnos sino el de comunicarnos de forma inmediata con otras personas.

Estos avances tecnológicos nos permiten, por un lado, tener una rapidez y continuidad de acceso a la información (antes inimaginables) y por el otro exponernos a otros riesgos que debemos conocer.

Estos riesgos quedan recogidos como medidas de actuación en el Plan Estratégico 2016/2019 en el marco del Observatorio de la Juventud de Aragón y nos posibilita a tener un conocimiento pleno de las nuevas inclinaciones que existen entre la Juventud de Aragón para poder responder con una mayor eficacia a sus necesidades y proposiciones.

Todo ello nos lleva a la creación de esta Carpeta de "Riesgos y amenazas en Internet y Redes Sociales" con el objetivo de sensibilizar, asesorar e informar a toda la comunidad educativa que trabajamos con y para los jóvenes.

Este documento explica los diferentes usos que se puede hacer de las redes sociales e internet, los virus que existen y las amenazas a las que estamos expuestos como usuarios/as de estas. Además, explica de una forma muy visual las distintas redes sociales y cómo utilizarlas. Para finalizar, consideramos muy adecuado poder hacer una guía de redes sociales que ayude a informar de las diferentes formas de seguridad que se pueden tener cuando nos damos de alta en cualquier red social.

Espero que este proyecto sea tan importante para todos/as vosotros/as como lo es para mí y podamos conseguir prevenir o erradicar el mal uso de las redes sociales y de internet.

Adrián Gimeno Redrado
Director Instituto Aragonés de la Juventud

1. Nuevas amenazas en la sociedad de la información 5

Medidas de proteccion contra virus (malware) 7
Otras amenazas en internet 9

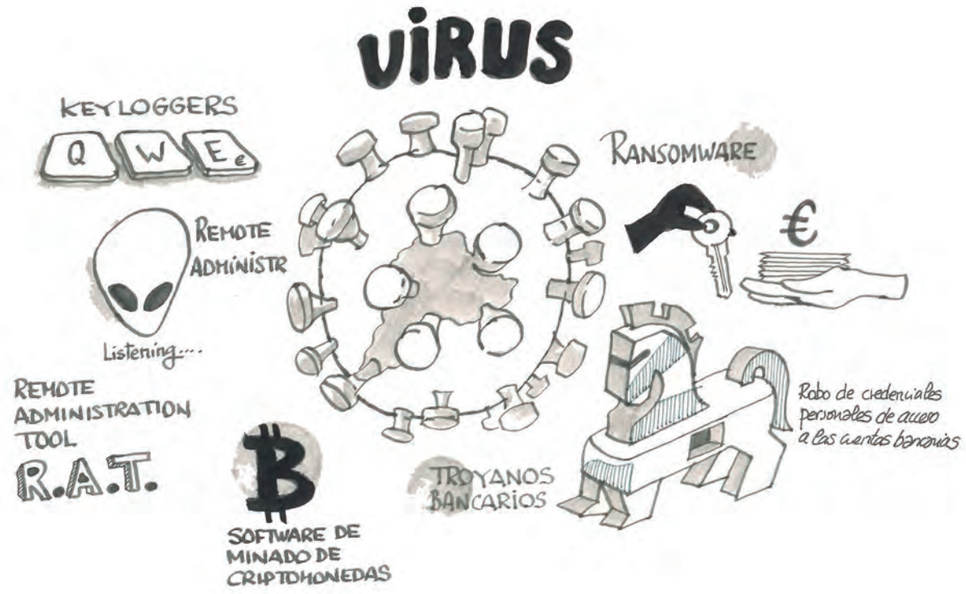
2. Telefonía móvil 11

Otro tipo de comunicaciones 14
Otros dispositivos conectados 14
Otras medidas de seguridad 15
Buenas prácticas y sugerencias a la hora de establecer contraseñas para nuestras cuentas 16

3. Servicios en la "nube" 18

¿Qué es la nube? 19
Redes sociales 24
Videojuegos - La amenaza latente 44

4. Guía de buenas prácticas 46



1 nuevas amenazas en la sociedad de la información

Para entender las amenazas que ponen en peligro la sociedad de la información, lo primero que hay que saber es qué es la sociedad de la información.

Desde los inicios de la informática e Internet, el objetivo de estas herramientas era crear un nuevo canal de gestión y comunicación de la información. La facilidad de uso y capacidad de trabajo de los ordenadores, iniciaron una revolución en la década de los 90 y principios del año 2000. Gracias a esta revolución tecnológica, la sociedad empezó a cambiar sus hábitos en lo referente a la búsqueda y consumo de información.

Empezaron a dejarse de utilizar las guías telefónicas, abriéndose paso los buscadores de Internet, como Yahoo! o Google. El correo tradicional fue dejando paso al e-mail, y las noticias ya no sólo se podían consultar en prensa, radio o televisión, sino que se empezaban a consultar mayoritariamente en Internet, debido a la inmediatez de su publicación.

Posteriormente a esta etapa, empezaron a surgir las redes sociales, aplicaciones basadas en la web, que conectaban personas de la misma facultad (así empezó Facebook), o permitían compartir información muy corta, pero de manera instantánea a nivel global (Twitter). Estaba empezando a cambiar la manera en la que nos relacionamos.

Esta primera revolución se produjo de manera relativamente lenta, para los tiempos que se manejan en las nuevas tecnologías, debido a que ni las redes de comunicación, ni los dispositivos con los que se accedía a Internet, tenían la potencia o portabilidad actuales.

Entonces llegaron los smartphones, y todo cambió.

Ya no era necesario llegar a casa para consultar las noticias o buscar información en Internet. Ahora podemos hacerlo con un simple gesto de la mano.

Dejo de ser necesario también llevar una cámara fotográfica encima, nuestro teléfono permite hacer fotografías con una calidad más que decente.

Tampoco necesitamos ya estar conectados a Internet a través de un cable y una línea telefónica, tenemos acceso en casi cualquier parte del planeta, sin necesidad de cables o dispositivos que nos den acceso.

Esta democratización del acceso a Internet, supuso su despegue e implantación definitivos, creando lo que conocemos como sociedad de la información. Un mundo hiperconectado en el que desde cualquier lugar se puede enviar cualquier información, y ser consultada instantáneamente de manera global.

Vivimos en la era de la información.

-Como puedes observar, todo se basa en la información, los ordenadores/tablets o smartphones son los encargados de generarla y procesarla. Internet sirve como hilo conductor de esta información, para hacerla llegar al destino deseado.

Y precisamente la información, es el objetivo número uno para los atacantes, y por lo tanto es aquello que debemos proteger, ya que es nuestra.

Desde el mismo inicio de la era de la sociedad de la información han existido los virus. Un virus es un software o programa informático, cuyo propósito es hacer que los dispositivos no funcionen de la manera en la que fueron pensados.

Al inicio, los virus eran creados con el afán principal de destruir, sin buscar ningún beneficio concreto. Ejemplos como el virus ILOVEYOU, generaron miles de millones de euros en pérdidas, ya que afectó a casi el 10% de los ordenadores conectados a Internet.

Durante la primera década del siglo XXI, los virus que circulaban por la red tenían casi en su totalidad la misma finalidad, destruir o inutilizar la información del ordenador que se veía infectado.

Los creadores, pocas veces se hacían públicos, y se empezó a crear la imagen de los "hackers". Individuos anónimos, con un gran conocimiento técnico, cuyo único objetivo era hacer daño, con diversos motivos, principalmente personales. Esta imagen ha perdurado hasta nuestros días, tapando de alguna manera la realidad a la que nos enfrentamos actualmente.

Hoy, prácticamente el 100% de los virus se programan con el objetivo de obtener un beneficio económico, bien directa o indirectamente. Por este motivo, las amenazas son cada vez más sofisticadas y elaboradas, pudiendo poner en peligro nuestra privacidad e intimidad.

Los tipos de virus más populares actualmente son:

• **Ransomware:** Un tipo de virus que cifra nuestros archivos personales, haciéndolos inaccesibles. Para poder recuperarlos, el delincuente solicita el pago de una cantidad a modo de "rescate", en teoría una vez realizado el pago, el atacante proporciona el medio para recuperar la información. En la práctica, esto ocurre en muy pocas ocasiones, habiendo realizado el pago y quedándonos sin acceso a nuestra información.

Para evitar caer en esta estafa, la práctica recomendada es la creación de copias de seguridad de nuestra información (fotos, videos, trabajos, documentos, etc...) en un soporte diferente al ordenador, pudiendo ser DVD, dispositivos USB como memorias flash o discos duros, o utilizando algún método de almacenamiento en la nube, como Dropbox o Google Drive.

• **Troyanos bancarios:** Este software está ideado para robar las credenciales personales de acceso a las cuentas bancarias. De esta manera, el atacante obtiene acceso a nuestro dinero, pudiendo realizar operaciones con nuestra cuenta a través de Internet. Este virus es muy peligroso, ya que generalmente somos conscientes de que hemos sido infectados cuando desaparece nuestro dinero.

• **Software de minado de criptomonedas:** Una criptomoneda es dinero virtual, el cual se genera a través de unas operaciones matemáticas complejas. Para llevar a cabo estas operaciones, es necesaria una gran capacidad de procesamiento de datos. La infraestructura para realizar estas operaciones, además del gasto energético que supone, hace que "minar" esta moneda sea muy costoso o muy lento sino se dispone de esa capacidad de procesamiento.

Es por este motivo que se han creado este tipo de virus, los cuales, una vez infectado un ordenador, comienza a usarlo para minar este tipo de moneda. Como efecto secundario para la víctima, se produce una ralentización del ordenador o del teléfono móvil, acortando su vida útil y en muchos casos impidiendo un uso normal del dispositivo.

• **R.A.T. Remote Administration Tool:** Este tipo de virus, conocido como Herramienta de Administración Remota, deja el ordenador de la víctima al servicio del atacante. De manera habitual este virus permanece "dormido" en el ordenador de la víctima, hasta que el atacante lo activa a través de un servidor central de mando y control. En ese momento, el atacante puede utilizar el ordenador infectado de la manera que quiera, aunque generalmente se utiliza como pieza para lanzar un ataque a gran escala a otras infraestructuras.

• **Keyloggers:** Este software almacena las pulsaciones del teclado, enviándolas posteriormente al atacante. De esta manera, es capaz de conocer cuáles son nuestras cuentas y sus respectivas contraseñas. En las versiones más avanzadas de este tipo de malware, se realizan también capturas de pantalla cada vez que se hace un clic con el ratón, de esta manera son capaces de conocer la contraseña, aunque se utilice un teclado virtual (teclado en pantalla).

Como vemos, los virus más populares ya no buscan realizar un daño directo a las víctimas, sino que las utilizan como medio para obtener un beneficio de manera directa o indirecta.

Por supuesto, las técnicas y herramientas utilizadas por los atacantes cada día son más sofisticadas y complejas, con el objetivo de evadir las medidas de seguridad existentes y conseguir sus propósitos.

Por este motivo, es muy importante que sigas los consejos de seguridad que proponemos a lo largo de la siguiente sección, ya que te librarán de más de un disgusto.

MEDIDAS DE PROTECCIÓN CONTRA VIRUS (MALWARE)

Como ya hemos visto, los virus, también conocidos como malware, se presentan de diversas formas y tienen objetivos diferentes. Lo que no cambia en ninguno de ellos es la manera en la que se propagan o infectan el ordenador de las víctimas.

Por eso es muy importante seguir unos consejos de seguridad básicos, con el objetivo de estar a salvo de la mayoría de infecciones que podemos sufrir.

- Actualizar siempre todo el software:

Los dispositivos, tanto ordenadores, como tablets y smartphones, necesitan programas para que ofrezcan funcionalidades a los usuarios. Dentro del software, se hace una clasificación según su funcionalidad:

-Sistema Operativo: Es el núcleo del dispositivo, el software más importante, ya que es el encargado de hacer funcionar todo lo demás de manera correcta. En ordenadores, el sistema operativo más popular es Windows, y en tablets y smartphones podemos encontrarnos con dispositivos cuyo sistema operativo es Android o IOS, en los dispositivos Apple.

Este software es crítico para el funcionamiento del dispositivo, por lo tanto, crítico también para la seguridad del mismo. Un sistema operativo sin actualizar es un objetivo prioritario para todo este software malicioso, ya que aprovechan "agujeros de seguridad" o bugs, para ejecutarse y producir sus efectos dañinos.

Por este motivo, es muy importante que mantengamos nuestros dispositivos actualizados a la última versión del sistema operativo, ya que cada nueva versión corrige los agujeros de seguridad detectados, además de ofrecer funcionalidades nuevas o mejoras en el rendimiento.

-Aplicaciones: Sin ellas, los dispositivos ofrecerían una funcionalidad limitada. Gracias a las aplicaciones podemos crear textos en un ordenador, hacer fotos con la cámara del móvil, o ver vídeos en una tablet.

Al igual que ocurría en los sistemas operativos, las aplicaciones también pueden tener fallos de

seguridad que permitan la propagación y ejecución de virus, por lo tanto, debemos preocuparnos de actualizarlas siempre a la última versión disponible, ya que sino quedaríamos expuestos a sufrir ataques de este tipo.

-Software antivirus:

Por supuesto, la protección debe ser lo primero que tengamos instalado en nuestros ordenadores. Si bien es cierto que la eficacia de los antivirus en dispositivos móviles aún está por probar, en ordenadores es de vital importancia tener un antivirus instalado y actualizado.

Es posible que la pieza de software que más necesite ser actualizada sea precisamente el antivirus, ya que las empresas creadoras de estos programas, actualizan prácticamente a diario la base de datos de virus, añadiendo la capacidad de detectar las amenazas más recientes y protegiéndonos contra ellas.

-Acciones del usuario:

Por último, tenemos que tener cuidado nosotros mismos como usuarios. En la actualidad, el vector de ataque más utilizado son las personas, ya que somos extremadamente vulnerables.

Los atacantes están buscando constantemente la manera de engañarnos, intentando que abramos un correo electrónico malicioso, que visitemos una página web o descarguemos en el ordenador o teléfono una aplicación fuera de los canales oficiales. Es por ese motivo que recomendamos la siguiente lista de acciones a evitar, para no caer en las trampas que nos ponen y evitar ser víctimas de virus:

-No abrir nunca correos electrónicos de desconocidos: En muchos casos los programas de correo filtran aquellos correos que pudieran ser maliciosos, pero como los atacantes están

constantemente evolucionando para evitar ser detectados, es posible que en ocasiones nos lleguen correos sospechosos.

Cuando recibamos correos que contengan archivos adjuntos de remitentes desconocidos o sospechosos, nunca debemos ni siquiera abrir el mensaje de correo, directamente eliminarlo.

En otras ocasiones, los correos no contendrán archivos, sino que tendrán uno o varios enlaces a páginas web. En este caso, nunca debemos pulsar en esos enlaces, ya que seguramente nos lleven a una página web que instalará el software malicioso.

Por último, aunque no menos peligroso, en ocasiones los atacantes intentarán hacerse pasar por una empresa u organización famosa (por ejemplo, un banco o una red social). Con el pretexto de mantener segura nuestra cuenta, o para comprobar que seguimos teniendo la cuenta activa, nos pedirán que introduzcamos nuestras credenciales de acceso, esto es, nuestro usuario y contraseña. **Nunca debemos hacerlo.**

Ninguna de estas organizaciones nos pedirá nunca nuestra contraseña, bajo ningún pretexto. Como puedes imaginar, están intentando robarnos nuestra contraseña, para poder acceder a nuestras cuentas, ya sean bancarias, de páginas web, redes sociales, etc...

Estos ataques reciben el nombre de **phishing**.

-Descargar aplicaciones sólo desde ubicaciones de confianza:

Las aplicaciones para teléfonos móviles son actualmente una de las vías de contagio más utilizadas. Para conseguirlo, los atacantes incluyen el virus en una aplicación legítima, y posteriormente la distribuyen fuera de los canales oficiales.

Como sabes, en Android el canal oficial es Play Store, y en IOS, la App Store e iTunes. Toda aplicación que instalemos que provenga de otro sitio que no sea un sitio oficial, tiene el riesgo de contener un virus.

Generalmente estas aplicaciones prometen funcionalidades extendidas para aplicaciones muy populares, o conseguir que ciertas funcionalidades de pago, las consigamos de manera gratuita.

En realidad, el precio que estamos pagando puede ser muy alto si nos vemos afectados por uno de estos virus.

-Enlaces en páginas web: Otro de los métodos más usados para extender virus son las páginas web de descargas. En muchas ocasiones, cuando se quiere descargar un archivo de Internet, además de la cantidad de publicidad que se nos presenta, aparecen botones de descarga los cuales no corresponden con la descarga real, estando el enlace correcto escondido entre varios de ellos.

Debemos ser muy cuidadosos a la hora de pinchar esos enlaces, ya que, de manera general, nos llevarán a sitios para instalar software no deseado en el ordenador, siendo en muchos casos virus o software espía.

Como vemos en esta imagen, al situar el ratón encima de un enlace (con el número 1 en la imagen), en la parte inferior del navegador nos aparece la dirección a la cual nos lleva dicho enlace si hacemos clic en él (el número 2 en la imagen). Debemos asegurarnos que el enlace nos lleva a la página que nosotros queremos, no a otra cuyo nombre pueda sonar extraño.

Resumiendo:

- Actualizar todo el software instalado, tanto sistema operativo como aplicaciones.
- Instalar y mantener actualizado el software antivirus.
- Ser cautos a la hora de abrir correos electrónicos
- No instalar aplicaciones provenientes de fuera de los canales oficiales
- Ser precavidos a la hora de pinchar enlaces web.

OTRAS AMENAZAS EN INTERNET

Los riesgos existentes en Internet, no sólo vienen de parte de virus y software malicioso. Como hemos dicho anteriormente, lo más importante es la información. Internet y los dispositivos que usamos para conectarlos a la Red, lo único que hacen es gestionar y transportar la información que se genera, y por supuesto, nuestra información también está incluida.

Dos de las amenazas a las cuales nos enfrentamos diariamente prácticamente sin saberlo son:

-Suplantación de identidad: Consiste en hacerse pasar por otra persona, habiendo obtenido con anterioridad sus datos personales. Los delincuentes utilizan la suplantación de identidad para realizar operaciones ilegítimas con otro nombre, dirección, etc... Puede darse el caso de que realicen compras a través de Internet utilizando los datos de nuestra tarjeta de crédito, práctica conocida como "carding".

-Doxing: Práctica consistente en obtener toda la información posible de una persona disponible en Internet. Para conseguirlo se utilizan tanto fuentes oficiales, como Boletines Oficiales, concursos públicos, etc... a través de sus páginas web, o utilizando la información disponible en redes sociales. Las consecuencias de esto pueden derivarse en casos de ciberbullying o acoso, y en publicación de información que puede causar un perjuicio a nuestra imagen y reputación.

Para estar a salvo de estas dos prácticas, debemos ser muy cautos a la hora de compartir nuestra información personal en Internet. En muchas ocasiones, tanto personas como aplicaciones web solicitarán nuestros datos personales, ya sea con la excusa de registrarnos en alguna aplicación o sitio web, o porque queremos contratar los servicios de algún profesional a través de Internet.

Debemos estar siempre alerta y comprobar que realmente la información que estamos proporcionando es adecuada al servicio en el que queremos registrarnos, y que la empresa o profesional que nos los demanda, cumple con todas las obligaciones que exige la ley, tanto en materia de protección de datos personales como en la información que tiene que proporcionar en base a la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico(LSSI).

Si en algún momento detectamos que podemos estar siendo víctimas de una estafa o están solicitando datos personales que nada tienen que ver con el servicio que están ofreciendo, debemos informar inmediatamente a la oficina de seguridad del internauta, www.osi.es, la cual nos dará pautas sobre las acciones que debemos tomar.

PÁGINAS DE DESCARGAS

Uno de los sucesos más sonados en la historia de Internet, y que sirvió para que la red llegará a muchísimas personas y alcanzara fama mundial fue el caso Napster.

Napster fue uno de los primeros programas que utilizaban las personas para descargarse música gratis, por supuesto, incluyendo música que estaba sujeta a derechos de autor. Este caso abrió un debate sobre la manera en la que se debían tratar los derechos de autor en la red, y de qué manera se tenían que evitar y sancionar estas prácticas.

Cuando Napster tuvo que dejar de ofrecer música gratis, tomaron fama los protocolos P2P (Peer to Peer) para el intercambio de ficheros. Este tipo de transferencia de ficheros no descargan los archivos desde un servidor central dónde se almacenan al resto de usuarios. Son los propios usuarios los que almacenan los archivos y los comparten con los demás miembros de la red.

De esta manera, las descargas no eran tan *ilegales*, porque se acogían al derecho de copia privada. Esto significa que, como los archivos (ya fueran música, películas, series, videojuegos, ...) no estaban controlados por una única persona que los distribuía de manera indiscriminada, sino que eran los usuarios los que se los pasaban de unos a otros, se consideraba que eran copias privadas, que están permitidas por la ley.

Sin embargo, no queda muy claro aún hoy en día que esta práctica sea totalmente licita, y es posible que, si hacemos uso de las páginas de descargas, algún día veamos el acceso a éstas bloqueado. Además, es posible que, en un futuro cercano, el hacer uso de estos servicios tenga consecuencias legales para nosotros. En otros países de nuestro entorno, como Francia o Reino Unido, ya se sanciona a los usuarios de este tipo de contenidos.

Software de pago protegido

Cuando queremos descargarnos un software de pago de manera gratuita, por norma general, el programa no funciona sino le ponemos un crack. Este crack lo que hace es saltarse las protecciones anticopia del software, y permite que se utilice sin tener que pagar nada a los creadores del programa.

Pero esto no quiere decir que a nosotros no salga gratis.

Actualmente, sobre todo para los programas más famosos y comerciales, las personas que realizan

estos cracks, necesitan invertir muchas horas, esfuerzo y conocimientos para conseguir que su crack funcione. ¿Crees que van a regalártelo?

Coinhive

Seguro que en los últimos meses habrás oído hablar más que nunca sobre las criptomonedas, moneda virtual que tiene valor real y puede ser usada para pagar, como por ejemplo el Bitcoin.

Para "fabricar" criptomonedas, es necesario que ordenadores muy potentes realicen cálculos muy complejos. Cuando este proceso se completa, "fabricando" por ejemplo un Bitcoin, el "minero" lo vende y obtiene dinero a cambio.

A finales del año 2017, principios del 2018, apareció la noticia de que muchas páginas web aprovechaban cuando eran visitadas, para que los ordenadores y móviles de los visitantes "minaran" criptomonedas para los dueños de la web, utilizando de esta manera los dispositivos para generar dinero, utilizando para ello un programa llamado Coinhive.

Gracias a este proceso, no se necesitaba mucho dinero para comprar ordenadores capaces de realizar las operaciones necesarias para el minado de criptomonedas, ni siquiera tenían que gastar la energía eléctrica requerida. Simplemente dejaban que los visitantes de la página web, hicieran el trabajo por ellos. Los visitantes notaban que cuando entraban a una web que utiliza este sistema, el rendimiento de su ordenador caía en picado, llegando incluso a quedarse "colgado".

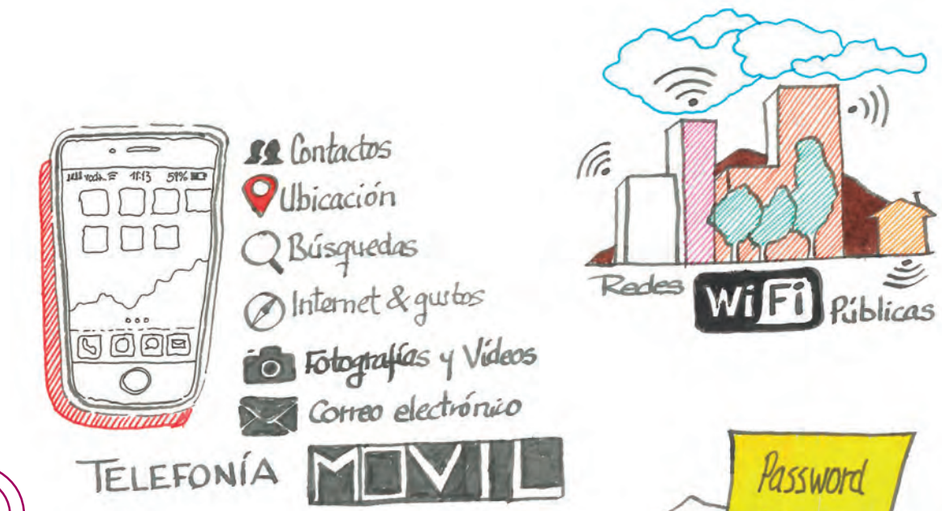
Aunque los efectos negativos son peores en los teléfonos móviles, los cuales no están preparados para realizar estos cálculos, llegando incluso a romperse por completo debido al calor generado al realizar estas operaciones.

En la mayoría, por no decir en absolutamente todos los cracks, seguro que se esconde algún tipo de malware. Puede ser un virus que nos monitorice la actividad en Internet, para posteriormente venderlo a terceras personas, pueden ser troyanos que nos roben los datos bancarios o los datos de acceso a nuestras cuentas, puede ser archivos que incluyan a nuestros dispositivos en botnets, que posteriormente se utilicen para lanzar otro tipo de ataques, etc...

Hay cientos de maneras en las que pueden utilizar nuestros dispositivos para obtener un beneficio, y nosotros estamos abriéndoles las puertas de par en par.

Así que, no sólo por este motivo, sino porque el software (pueden ser programas de edición fotográfica, programas ofimáticos o videojuegos) lo realizan personas, las cuales invierten mucho tiempo en formarse, mucho tiempo en desarrollar, depurar y adaptar el software para que podamos utilizarlo. Cuando descargamos software de manera ilegal, lo que estamos haciendo es negar a esas personas la recompensa por su trabajo.

Por lo tanto, piensa bien las implicaciones que tiene descargar contenido de Internet, tanto para los demás como para tu seguridad.



2 telefonía **móvil**

Aunque muchas de las amenazas que ya hemos ido enumerando, afectan tanto a ordenadores personales como a smartphones, el hecho de que estos últimos se hayan incorporado de manera masiva a nuestro día a día, ha generado todo un ecosistema de amenazas y riesgos que afectan de manera principal a este tipo de dispositivos.

Además, el uso que hacemos de ellos es mayoritario en comparación con el uso que hacemos de los ordenadores personales, que han quedado relegados a un uso más académico y profesional o de ocio electrónico.

Debido al uso cada vez más extenso que hacemos de los smartphones, los delincuentes y usuarios malintencionados han puesto su foco en estas plataformas, esperando poder encontrar un mayor número de víctimas, aprovechando además la facilidad de acceso a ellos y la simplicidad de su uso.

Los smartphones, al ser utilizados prácticamente en exclusiva de manera personal almacenan grandes cantidades de información sobre nosotros.

Esta información abarca:

- Datos de nuestras redes sociales.
- Contactos.
- Ubicación.
- Búsquedas en Internet.
- Intereses y gustos en función de las aplicaciones instaladas.
- Fotografías y vídeos.
- Conversaciones privadas.
- Correo electrónico.
- Videojuegos.
- Agenda personal.

Toda esta información resulta muy interesante para los delincuentes, la cual puede usarse para que obtengan un beneficio, o para causarnos un perjuicio.

CASO POKEMON GO

Cuando apareció el videojuego Pokemon GO, supuso una pequeña gran revolución en la manera en la que se jugaba con los smartphones. Dando el salto a la realidad aumentada, el juego propone el salir a la calle a cazar *pokémons*, y añadirlos a nuestra colección.

Este videojuego utiliza dos de las funciones propias de los smartphones, la geolocalización y la cámara de fotos.

Además, los creadores del juego, quisieron añadir cierto componte social, al añadir los cebos. Este objeto, una vez utilizado dentro del juego, hace que los

pokémons acudan al punto geográfico donde se ha situado, haciendo que los demás entrenadores acudan a él para encontrar más *pokémon* que añadir a su colección.

En muchas ciudades del mundo, se han organizado grupos para salir a cazar estos pokémon, ubicando en varios puntos de la ciudad cebos, para que los participantes realicen rutas a lo largo de parques, avenidas, etc...

Cuando el juego llevaba poco tiempo en el mercado, saltó la noticia de que delincuentes comunes, situaban cebos en calles apartadas y desprotegidas. Cuando un jugador se acercaba en busca de más *pokémon*, los delincuentes lo asaltaban, robándole sus pertenencias reales.

Este ejemplo, da una idea clara de cómo una funcionalidad aparentemente inofensiva, y que además promueve un juego social y participativo, puede ser usada de manera malintencionada, poniendo en riesgo no ya sólo nuestra privacidad, sino nuestra seguridad física.

En los teléfonos móviles, además, existe la posibilidad de incluir en las fotografías información sobre la ubicación en la que se ha realizado la fotografía. Esto es, nuestras fotos están geolocalizadas. Por lo tanto, cualquier usuario que se haga con una copia de esta imagen, puede saber en qué momento y dónde ha sido tomada.

Esto puede dar pistas a un delincuente sobre nuestros horarios, hábitos, rutas, incluso sobre cuándo no estamos en casa, o cuándo y a dónde nos vamos de vacaciones.

Por eso es muy importante desactivar todos los servicios de geolocalización de los smartphones, excepto cuando realmente vayamos a hacer uso de ellos, por ejemplo, a la hora de utilizar el GPS para ubicarnos o buscar una dirección en un mapa, o cuando realmente sepamos que la información que vamos a compartir, únicamente va a ser en nuestro grupo de confianza (amigos cercanos y familiares).

-App´s Maliciosas

No sólo los virus se esconden en aplicaciones obtenidas fuera de los canales oficiales. Actualmente las grandes empresas del sector como Google o Apple, luchan por detectar y eliminar de estos canales aplicaciones que aparentan ser legítimas, pero que realmente esconden software malicioso en su interior.

Afortunadamente, ambas compañías trabajan de manera proactiva para proteger nuestra privacidad, y ponen a nuestra disposición herramientas que nos pueden ayudar a identificar este tipo de aplicaciones.

La manera más útil y común de hacerlo, es revisar los permisos que nos solicitan a la hora de instalarlas.

En muchas ocasiones, las aplicaciones maliciosas necesitan permisos especiales para conseguir su objetivo. Por ejemplo, deberíamos sospechar de una aplicación que instale un nuevo tipo de teclado en nuestro teléfono, y pida permisos para acceder a nuestros contactos.

O un videojuego que necesite acceder a nuestro almacenamiento local y **enviar y recibir SMS,** es algo que puede hacernos pensar que esa aplicación en concreto esconde algo más.

Otra de las formas para detectar aplicaciones fraudulentas es a través de las valoraciones y los comentarios dentro de la propia plataforma. El hecho de que una aplicación tenga muy pocos comentarios o valoraciones, y todos ellos sean positivos o muy positivos, puede ser un indicador de que se han falseado los comentarios, con el objetivo de hacer parecer legítima la aplicación.

Además, comprobar cuál es la empresa desarrolladora, y asegurarnos de que sea un desarrollador de confianza, son indicios de que la aplicación es legítima y no contendrá malware de ningún tipo.

Redes Wi-Fi públicas

Hoy en día es muy común que durante el mes se nos agote nuestro plan de datos móviles, y busquemos constantemente redes Wi-Fi de acceso público. Independientemente de que la red tenga o no contraseña, debemos ser extremadamente cautos a la hora de utilizar este tipo de conexiones.

Uno de los ataques más antiguos, y todavía en vigor, hace uso de una técnica llamada Man-In-The-Middle, con el objetivo de espiar todas las comunicaciones que se realizan desde nuestros dispositivos.

En una red Wi-Fi privada, en la cual sólo nosotros conocemos la contraseña, es relativamente difícil ser víctimas de este tipo de ataque, sin embargo, en espacios públicos como cafeterías, bibliotecas, centros comerciales, etc... sí que es muy fácil conseguir realizar este tipo de ataque, el cual además no requiere de grandes conocimientos técnicos.

En el momento en el que un atacante empieza a espiar los datos que circulan a través de una red, es capaz de ver toda la información que estamos enviando y recibiendo. De esta manera puede llegar a ser capaz de conocer nuestras contraseñas, números de tarjeta de crédito, etc...

Para evitar en la medida de lo posible este tipo de ataque, debemos ser muy cuidadosos a la hora de enviar información a través de este tipo de redes.

Teniendo en cuenta que debemos evitar en todo momento acciones como:

- Acceder a páginas web con nuestra contraseña
- Acceder a webs o aplicaciones que no cifren el tráfico
- Enviar información sensible como fotografías o datos personales

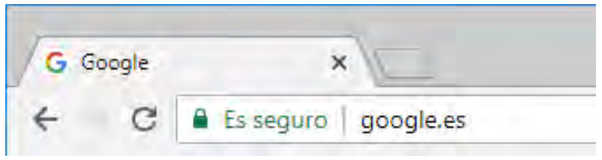
HTTP Vs HTTPS

HTTP o Hypertext Transfer Protocol (protocolo de transferencia de hipertexto), es el estándar por el cual funciona toda la Web. Es uno de los protocolos más antiguos de Internet, y cuando se desarrolló no se tuvo en cuenta la privacidad de las comunicaciones, ya que su desarrollo se realizó en redes muy pequeñas y controladas. Cuando utilizamos páginas web que usan este protocolo, toda la información que enviamos y recibimos es en texto plano, es decir, cualquier persona que intercepte esa comunicación puede saber la información que estamos enviado y la que estamos recibiendo.

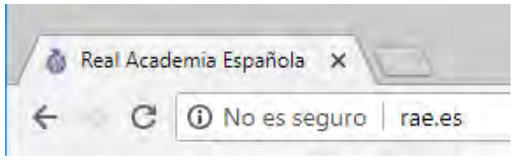
Por lo tanto, cualquier petición que realicemos a un sitio web, podrá ser consultada por cualquiera que este espiando la red a la que estamos conectados. Esto incluye contraseñas, información bancaria, personal, imágenes, etc...

Para evitar este tipo de ataques, posteriormente se desarrolló el estándar HTTPS o Protocolo de transferencia segura de hipertexto. En este estándar, las comunicaciones entre nuestro dispositivo y la página web que estamos consultando permanecen cifradas, por lo tanto, cualquier espía que esté en nuestra red, no será capaz de saber qué información estamos intercambiando.

Actualmente, las diversas organizaciones que componen Internet están trabajando para que, en un futuro, todas las páginas web existentes en Internet utilicen este protocolo para sus comunicaciones. Hasta que llegue este momento, debemos ser nosotros los que consultemos si las comunicaciones se realizan cifradas o sin cifrar.

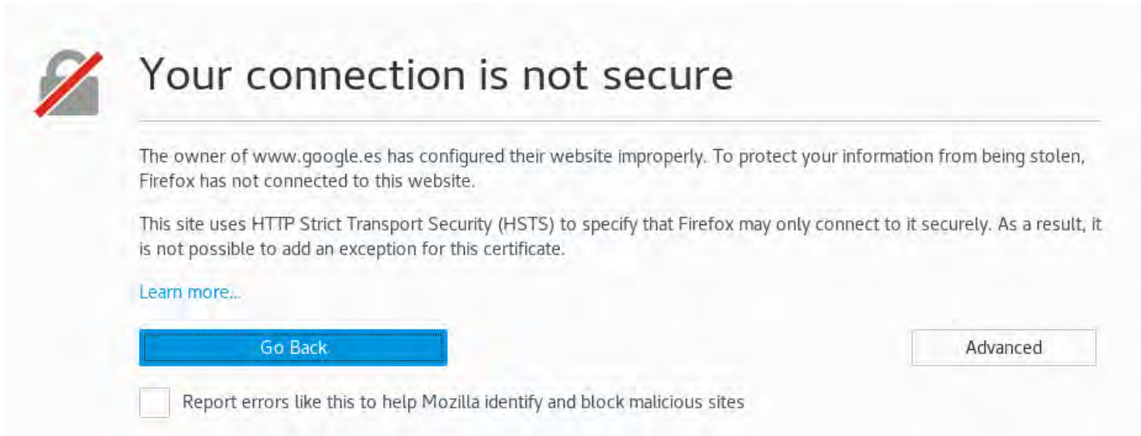


Esta web usa cifrado



Esta web no usa cifrado

Aunque este método es bastante seguro, los atacantes tienen métodos para intentar burlarlo, si estando conectado en una red pública, intentas acceder a una página web con normalidad y aparece este mensaje:



Cierra la sesión inmediatamente, porque podría significar que alguien está intentando espiar tus comunicaciones.

OTRO TIPO DE COMUNICACIONES

En nuestros teléfonos móviles, no sólo existe la red de voz/datos y la red Wi-Fi. También incorporan otro tipo de protocolos de comunicación, útiles para diversos servicios o dispositivos complementarios, como por ejemplo la tecnología Bluetooth o NFC.

Estos protocolos de comunicación, aunque bastante recientes, se desarrollaron en una época en la que se consideraba que la distancia era una medida de seguridad.

Es decir, cómo son comunicaciones muy próximas, era muy difícil que un atacante pudiera interceptar la comunicación y espiar el contenido de lo que se transmitía utilizando estas tecnologías.

Pero como ya sabes, los atacantes intentan ir siempre un paso por delante, y actualmente son protocolos de comunicación que se consideran INSEGUROS.

Es por este motivo que sólo debemos activar el bluetooth o el NFC de nuestros teléfonos en el momento en el preciso momento en el que lo vayamos a utilizar, para desactivarlo inmediatamente después.

Con la llegada de los dispositivos llamados wearables, como relojes inteligentes, el uso de la tecnología bluetooth se está expandiendo. Para que estos dispositivos funcionen de manera correcta, debemos mantenerlos vinculados a un dispositivo móvil el 100% del tiempo, esto genera grandes dudas sobre la seguridad de la información que enviamos entre estos dispositivos y nuestro terminal.

Por ese motivo se recomienda que no se utilicen como medida de seguridad, por ejemplo, para desbloquear nuestro terminal si se encuentra cerca de un dispositivo bluetooth determinado. El rango óptimo de bluetooth son aproximadamente 10 metros, pero se han llegado a medir hasta 20 o 30 metros de alcance. Esto quiere decir que, si robaran nuestro dispositivo, ¡sería posible desbloquearlo desde fuera de nuestra casa!

OTROS DISPOSITIVOS CONECTADOS

Actualmente, no sólo los dispositivos de los que hemos estado hablando son objetivo para los atacantes, otros dispositivos que dan servicio de Internet, como los routers domésticos, o aparatos como SmartTV´s también han pasado a ser objetivos muy interesantes para los atacantes.

En muchas ocasiones, los métodos para estar protegidos requieren elevados conocimientos técnicos, ya que son dispositivos muy especializados que dan un servicio específico, aunque eso no significa que no podamos hacer nada para protegernos.

En general, es recomendable reiniciar un router doméstico una vez a la semana. De esta manera, si se ha visto comprometido, es posible que al realizar esta operación nos libremos del atacante. Por otro lado, apagarlo cuando no está en uso durante un largo periodo de tiempo, acorta la ventana temporal disponible para lanzar un ataque sobre él.

Respecto de los routers, es muy importante desactivar el acceso WPS, esto se puede realizar fácilmente y en caso de dudas, consultar con nuestra operadora de servicios de Internet, para que nos indique los pasos a realizar.

También es muy conveniente modificar la clave WPA ("la clave del Wi-Fi") que viene por defecto, por otra que sólo conozcamos nosotros y que sea difícil de adivinar. Para cada modelo de router, la configuración se hace de una manera diferente, por eso, para llevar a cabo estas operaciones lo mejor es contactar con nuestra operadora de servicios de Internet, para que nos indique los pasos a realizar.

De esta manera pondremos las cosas más difíciles a los atacantes.

En el futuro veremos miles de dispositivos conectándose a Internet, desde relojes, zapatillas, pulseras, hasta lavadoras, frigoríficos e incluso nuestra propia casa. Las recomendaciones de seguridad que hemos dado en este último apartado, se aplican perfectamente a todos estos aparatos, y son consideradas medidas de autoprotección, útiles para cualquier dispositivo conectado a Internet, sea cual sea su propósito.

OTRAS MEDIDAS DE SEGURIDAD

Ya hemos hablado de medidas de seguridad como antivirus, y medidas de precaución a la hora de navegar por Internet, descargarnos apps o conectarnos a redes Wi-Fi de acceso público.

Todas estas medidas de seguridad no sirven de nada, si no protegemos lo más importante, el acceso a nuestras cuentas.

¿Te imaginas dándole la llave de tu casa a un desconocido?, ¿prestándole el móvil a la primera persona que pase por la calle?, ¿dejarías entrar a tu casa a cualquier persona?

Tu identidad digital se define como toda aquella información que hay publicada en Internet sobre ti.

De tu identidad digital, la parte más importante la componen las cuentas que creas para acceder a servicios en línea, como redes sociales, páginas web, etc...

¿Imaginas qué pasaría si alguien pudiera acceder a todos tus perfiles de redes sociales, cuentas de aplicaciones web, y pudiera modificar o añadir el contenido que quisiera?

¿Qué crees que podría hacer un delincuente que tuviera acceso a tu cuenta de correo?

Podrían destruir completamente tu identidad digital, o podrían modificarla, incluso podrían bloquear tu acceso a todas tus cuentas, incluyendo la cuenta de correo, perdiendo el acceso a toda la información que existe sobre ti en Internet.

Actualmente, para proteger todo esto, el método más usado y común es la contraseña. Como ya sabes, la contraseña es un conjunto de caracteres, los cuales en teoría sólo deberías conocer tú, y que, junto a tu nombre de usuario, te identifican en un servicio o aplicación, permitiendo su uso.

Las contraseñas son las **llaves de tu casa en Internet.**

Ahora, repetiremos las preguntas anteriores, cambiando una palabra:

¿Te imaginas dando la contraseña a un desconocido?, ¿dándole el pin de tú móvil?, ¿dejarías tu cuenta de Facebook a cualquier persona?

Como vemos, las contraseñas son lo único que nos protege de accesos no autorizados a nuestras cuentas on-line.

Para comprobar la fortaleza de tus contraseñas, te invitamos a que realices el siguiente test:

¿Cuántos caracteres tiene tu contraseña?

A. Más de 10
B. Entre 7 y 10
C. 6 o menos

¿Utilizas letras mayúsculas y minúsculas?

A. Sí, y también números y caracteres especiales
B. Sí
C. No, todas son minúsculas, aunque añado números o caracteres especiales

¿Tu contraseña contiene algún dato personal? (Nombres de familiares, fechas de nacimiento, grupos de música favoritos, deportes, etc.)

A. No, las contraseñas que suelo utilizar son cadenas de texto aleatorias
B. No, pero utilizo palabras del diccionario
C. Si, suelo utilizar datos de ese estilo

¿Utilizas la misma contraseña para varios servicios o aplicaciones?

A. No, para cada cuenta que creo utilizo una contraseña diferente
B. Si, aunque añado pequeñas variaciones
C. Sí, siempre utilizo la misma contraseña

Mayoría de respuestas A: Enhorabuena, haces un uso responsable y coherente de las contraseñas. Además, en caso de que una cuenta sea vulnerada, las demás cuentas no se verán afectadas, ya que utilizas una contraseña diferente para cada servicio.

Mayoría de respuestas B: Utilizas contraseñas débiles, un atacante sería capaz de vulnerar tus contraseñas con relativa facilidad.

Mayoría de respuestas C: Estas en grave peligro. Debes adoptar una política de contraseñas más responsable, ya que en cualquier momento todas tus cuentas se pueden ver comprometidas, además de perder el acceso a ellas.

BUENAS PRÁCTICAS Y SUGERENCIAS A LA HORA DE ESTABLECER CONTRASEÑAS PARA NUESTRAS CUENTAS

Las contraseñas son quizás el elemento de seguridad que menos ha evolucionado desde su existencia. Generalmente tendemos a utilizar contraseñas fáciles de recodar y bastante simples, con el objetivo de no perder el acceso a nuestras cuentas. Incluso en muchas ocasiones, no protegemos el acceso a nuestros dispositivos como ordenadores o móviles, con un patrón de desbloqueo o contraseña.

Tampoco solemos cambiar las contraseñas que vienen establecidas por defecto en dispositivos como routers, SmartTV´s y demás dispositivos conectados a Internet (Lo que se conoce como el Internet de las Cosas).

Esta falta de responsabilidad a la hora de proteger el acceso a nuestra información, es un punto de entrada ampliamente utilizado por los delincuentes y usuarios malintencionados. Por eso, es muy importante tener claro que las contraseñas suponen la última barrera de protección frente a un ataque, y que deben de ser capaces de proteger nuestra privacidad y nuestra seguridad.

Para generar una contraseña robusta, difícil de adivinar y fácil de recordar, proponemos los siguientes consejos:

-Cantidad antes que calidad: Es muchísimo más difícil de adivinar una contraseña muy larga, que una contraseña corta que contenga caracteres especiales. Por ejemplo, la contraseña UjRt56* tiene 7 caracteres de longitud, conteniendo mayúsculas, minúsculas, números y caracteres especiales.

Un usuario que quisiera "romper" esta contraseña para acceder a nuestra información probando todas las posibilidades, tendría que comprobar 69.833.729.609.375 posibles combinaciones.

Sin embargo, si usáramos la contraseña: "el caballo blanco de santiago", las posibles combinaciones serían tantas como 236.773.830.007.967.588.876.795.164.938.469.376.

Y, sin embargo, ni se han usado mayúsculas, ni números, existiendo de hecho un único carácter especial, el espacio.

Por otro lado, la segunda contraseña es bastante más fácil de recordar que la primera, facilitando su uso y sin tener que apuntarla en ningún sitio.

Por supuesto, frases de este estilo son relativamente fáciles de adivinar, si en ellas utilizamos elementos comunes de nuestra vida, como, por ejemplo: "mi madre se llama paz y mi padre pedro".

Esta contraseña, aunque por longitud sería extremadamente segura, incorpora elementos fácilmente adivinables por un atacante, por lo tanto, perdería eficacia.

Es por este motivo, que debemos añadir **entropía** a la generación de contraseñas, esto es, **un componente aleatorio** que impida a un atacante adivinar la contraseña que hayamos elegido.

Por ejemplo, podemos usar estrofas de canciones, o agrupar elementos que no tengan relación para generar ese componente aleatorio: "el boli tiene un árbol verde en casa", es una frase que no tiene ningún sentido, por lo que es muy difícil de adivinar y, además, tiene la suficiente longitud como para no poder ser obtenida por "fuerza bruta".

El siguiente problema con el que nos encontramos en el uso de contraseñas es la reutilización. Es decir, usamos la misma contraseña para muchos servicios. Esta práctica, muy extendida, nos sitúa en un contexto de alta vulnerabilidad, ya que, si uno de estos servicios se ve comprometido y nuestra contraseña expuesta, inmediatamente el atacante podría acceder a todas y cada una de nuestras cuentas.

Es por este motivo que es muy importante tener una contraseña diferente para cada cuenta que creemos, diferenciándolas lo suficiente como para que no sean adivinables unas respecto de las otras (Si, por ejemplo, hemos utilizado la contraseña "el caballo blanco de santiago" para una de nuestras cuentas, no utilizar la contraseña "el caballo verde de santiago" para otra).

Cuando la cantidad de servicios en los que estamos dados de alta, se vuelve difícil de manejar, es posible que sea útil utilizar un programa o servicio de gestión de contraseñas. Este tipo de aplicación, almacena todas nuestras contraseñas cifradas, pudiendo acceder a ellas a través de una única contraseña, también llamada **contraseña maestra.**

Este tipo de aplicaciones son muy usadas para almacenar muchas contraseñas de diferentes servicios y de una gran complejidad, ya que sólo tendremos que acordarnos de la contraseña maestra. El gran problema de la utilización de esta solución, es que, si perdemos esa contraseña maestra, o alguien llega a conocerla, tendrá inmediatamente acceso a todas nuestras cuentas.

Por eso, a la hora de seleccionar la contraseña maestra, es muy importante seguir todas las recomendaciones a la hora de la creación de contraseñas, manteniendo una longitud grande y utilizando la mayor cantidad posible de caracteres diferentes.

Si quieres comprobar si una de tus contraseñas ha sido comprometida, puedes utilizar el servicio web https://haveibeenpwned.com/. Gracias a este servicio, introduciendo nuestro el correo electrónico que utilizamos al registrarnos en diferentes páginas web, nos dirá si ha aparecido en algún listado público de contraseñas, permitiéndonos conocer si hemos sido vulnerados o no.

Es importante consultar de manera periódica esta página web, para comprobar si nuestras cuentas se han visto comprometidas y poder actuar en consecuencia.

¿Qué hacer cuando nos roban o descubren nuestras contraseñas?

Casi a todos nos ha pasado alguna vez, que hemos perdido el acceso a una cuenta, o nos están llegando correos electrónicos de alguna newsletter a la que no nos hemos suscrito, o están empezando a aparecer publicaciones extrañas en nuestras redes sociales, las cuales no hemos publicado nosotros.

En esos casos, lo más probable es que nuestra cuenta haya sido vulnerada a través de nuestra contraseña, y lo único que podemos hacer es no perder la calma. Lo primero que debemos hacer, es cambiar la contraseña de nuestro correo electrónico. Tal y como funcionan ahora los servicios, es la llave para recuperar el acceso a cualquier cuenta que nos hayamos creado, por lo que, si perdemos el acceso a nuestra cuenta de e-mail, las cosas se complicarán un poco más.

Una vez que hayamos cambiado la contraseña de nuestra cuenta de correo, cambiamos la contraseña de la cuenta que nos hayan robado. En el caso de que el atacante haya podido cambiar la contraseña y no pudiéramos acceder, utilizando los formularios de recuperación de contraseñas, podríamos recuperar el acceso, y cambiar la contraseña.

Por último, deberemos cambiar TODAS las contraseñas de TODAS las cuentas a las que tengamos acceso. Esta medida de precaución está basada en que, si han conseguido acceder a una cuenta, ¿qué les impide acceder a las demás? De la misma manera que consiguieron el primer acceso, podrían haber conseguido más contraseñas o acceder a más de nuestras cuentas.

Una vez terminado todo el proceso, si se han seguido los consejos de creación de contraseñas que hemos dado en esta sección, volveremos a tener nuestras cuentas seguras.

Medidas adicionales de seguridad y buenas prácticas en el uso de contraseñas

Actualmente, existen mecanismos que nos permiten aumentar la seguridad de nuestras cuentas. Por ejemplo, la autenticación de doble factor.

Este tipo de autenticación necesita la realización de dos pasos para concedernos acceso. Generalmente, una vez que se ha introducido el usuario y la contraseña, nos enviarán un código a nuestro teléfono móvil o correo electrónico, y nos pedirán que introduzcamos ese código de un solo uso para acceder.

De esta manera, alguien que hubiera adivinado o conocido nuestra contraseña, todavía necesitaría acceso a nuestro correo electrónico o teléfono móvil para entrar en ella.

Como ventaja añadida, este servicio nos sirve de alerta, ya que, si en un momento en el que no estamos intentando nosotros iniciar sesión en una página web, y sin embargo nos llega la solicitud de autenticación de doble factor, sabemos que alguien está intentando entrar en nuestra cuenta, y que muy posiblemente conozca nuestra contraseña. Por lo tanto, deberemos cambiarla antes de que pudieran conseguir acceso por otros medios.

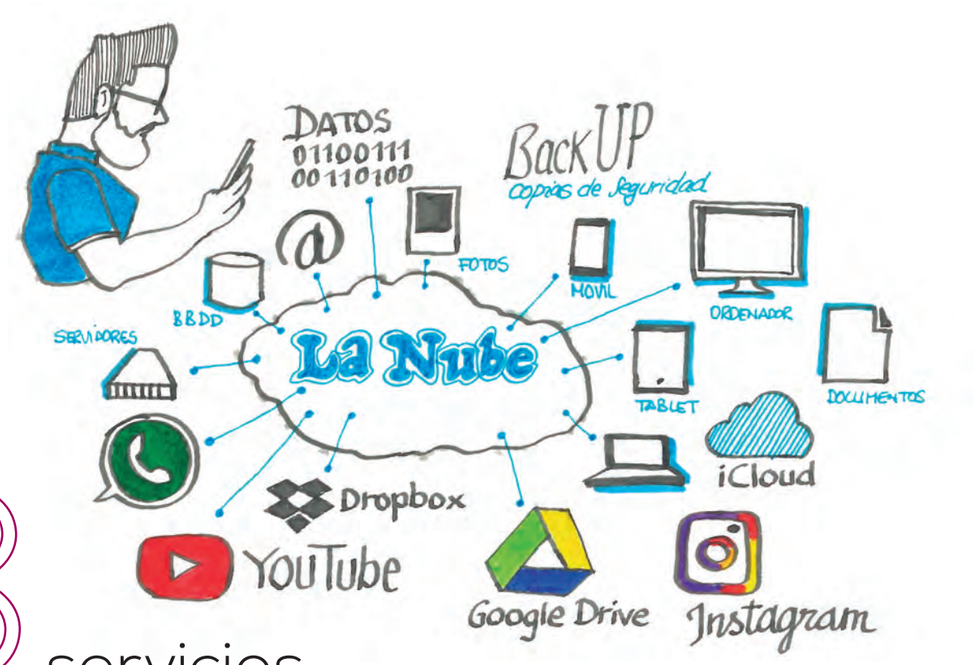
Otro tipo de autenticación que se está usando mucho, y cuya utilización es muy probable que aumente en el futuro, es la autenticación por Open ID. Este tipo de autenticación, usa los datos ya existentes de una cuenta, como por ejemplo nuestra cuenta de Google o Facebook, para crear una cuenta en otra aplicación o página web.

De esta manera, nuestros datos de acceso se encontrarán siempre en el mismo sitio, y no tendremos que estar introduciendo nuevas contraseñas para cada servicio o aplicación que queramos utilizar.

Por supuesto, en caso de utilizar este sistema de autenticación, es muy importante que la contraseña de acceso a la cuenta maestra sea muy robusta y no sea conocida por nadie.

Otra de las medidas de seguridad respecto de las contraseñas que tiene un uso poco extendido es la renovación. Generalmente, cada 3 o 4 meses deberíamos cambiar nuestras contraseñas, por precaución. De tal forma que si en algún momento de ese periodo, nuestra contraseña se viera comprometida, sólo lo estaría el tiempo que tardásemos en volver a cambiarla.

Si bien es cierto que esta práctica es poco cómoda, ya que nos obliga a crear y memorizar cada poco tiempo nuevas contraseñas, sí que deberíamos aplicarlo en las contraseñas más críticas, por ejemplo, con las contraseñas maestras de los gestores de contraseñas, o las que nos den acceso a servicios que tengan Open ID, como la contraseña de nuestra cuenta de Google o de Facebook.



3 servicios en la **"nube"**

Como ya hemos expuesto, Internet no sólo ha permitido acceder a una cantidad enorme de información casi en tiempo real, sino que, además, ha traído muchos servicios nuevos los cuales utilizamos casi a diario. Estos servicios o aplicaciones, son los que han conseguido que Internet sea una herramienta muy útil tanto para nuestros trabajos y estudios, como para nuestra vida personal. Ha conseguido modificar nuestros hábitos de consumo, nuestra forma de escuchar música, de ver televisión o incluso de relacionarnos con los demás.

Todas estas nuevas herramientas y servicios que utilizamos a diario desde nuestros ordenadores o nuestros móviles se han convertido en parte de nuestras vidas, y debemos aprender a hacer un uso responsable de las mismas.

Internet simplemente es la autopista por la que circula toda esta información, permitiéndonos acceder a ella, pero tenemos que ser plenamente conscientes de que al otro lado de la pantalla no hay sólo caracteres, imágenes o vídeos, sino que hay **personas**.

Personas que trabajan constantemente por que todo esto funcione, personas que se están encargando de crear nuevos servicios, herramientas y programas que faciliten más nuestra vida diaria o nos proporcionen más y mejores momentos de ocio. Hay personas que se relacionan con nosotros, que van a nuestras clases, institutos y trabajos. Personas que viven en nuestra misma calle o al otro lado del mundo.

Pero también hay personas cuyos intereses no son saludables. Personas que buscan obtener beneficio personal aprovechando el anonimato y la sensación de seguridad que da cometer un delito desde sus casas. Personas que utilizan la Red y sus servicios para sus actividades ilegales, y que, en un determinado momento, pueden utilizarnos a nosotros, como usuarios de estos servicios, para sus fines ilícitos, ya sea de manera directa o indirecta.

Es por esto, que para conseguir tener en Internet una experiencia de uso agradable y que sea fructífera y acorde con nuestros intereses, debemos tomar una serie de precauciones para permanecer a salvo de estos usuarios malintencionados.

Durante el primer bloque de esta carpeta, hemos comprobado las herramientas que pueden usar los atacantes para obtener beneficio a partir de virus y software malicioso. En este segundo bloque, veremos todas aquellas acciones que pueden realizar estos atacantes para engañarnos, chantajearnos o extorsionarnos, buscando un beneficio personal o simplemente por hacernos daño.

Y, sobre todo, no olvides que Internet es un sitio fantástico donde hacer nuevas amistades, conocer otros países o saber más acerca de cualquier tema que te interese, sin correr riesgo alguno, siempre que sigamos unas sencillas normas de uso.

¿QUÉ ES LA NUBE?

El concepto "nube" empezó a nombrarse a finales de los años 80, cuando Internet estaba dando sus primeros pasos tal y como lo conocemos hoy en día.

Los ingenieros encargados de diseñar las primeras redes de datos, solían representar Internet como una nube, con el objetivo de simbolizar toda una infraestructura muy compleja que interconectaba unos ordenadores con otros.

De esta manera, cuando se enviaba un correo electrónico a un ordenador remoto, se decía que el mensaje atravesaba la "nube" antes de llegar a su destino.

Este concepto ha llegado a nuestros días, y hoy la nube representa no ya sólo toda la compleja infraestructura de las autopistas de Internet, sino que también hace referencia a todos aquellos servicios o aplicaciones, a los cuales se accede a través de Internet.

Servicios como Dropbox, Google Drive o iCloud, ofrecen almacenamiento en la "nube". Lo que quiere decir que almacenan nuestros archivos en servidores remotos, a los cuales podemos acceder a través de Internet en cualquier momento o lugar. Cuando subimos una foto a este tipo de servicios, decimos que hemos "subido la foto a la nube".

Pero no sólo estos servicios de almacenamiento componen la "nube", cualquier aplicación que se ejecute en una página web, también lo está haciendo en la nube. Por ejemplo, Facebook, es una aplicación que se ejecuta en la nube. También YouTube, Instagram, incluso WhatsApp, es un servicio que se ejecuta en la nube.

Este método de trabajo, útil para tener siempre disponible nuestra información y accesible desde cualquier dispositivo o lugar, también lleva consigo un riesgo, del cual tenemos que ser conscientes. En el momento en el que subimos un documento, ya bien sea una foto, un vídeo, un trabajo, etc..., a la nube, inmediatamente perdemos el control sobre esa información.

Es decir, si publicamos por error una foto en Facebook o Instagram, y la borramos de manera inmediata, no podemos asegurar nunca más que no exista otra copia de esa foto.

Por este motivo, es **muy importante** ser conscientes de qué información almacenamos en la nube, y sobre qué información queremos mantener el control.

Además, el uso del almacenamiento en la nube, como único sistema de copias de seguridad, tampoco es recomendable, ya que el perder acceso a la cuenta, o una suspensión del servicio en el cual la almacenamos, haría que perdiéramos toda la información guardada, sin posibilidad alguna de recuperarla.

Por lo tanto, debemos ser conscientes de la información que almacenamos en estos servicios, así como la información que compartimos o enviamos utilizando herramientas que trabajen en la nube, puesto que nunca podremos saber con total seguridad, qué ha sido de nuestra información una vez se ha enviado.

REDES SOCIALES

Las redes sociales son aplicaciones basadas en la nube, las cuales han cambiado por completo la manera en la que nos relacionamos.

Hasta la aparición de Facebook, la red social más conocida hasta la fecha, la interacción de los usuarios de Internet se hacía de manera anónima en chat´s y foros de Internet conocidos como news.

IRC, Grupos de NEWS y MSN Messenger

IRC son las siglas de Internet Relay Chat, el protocolo utilizado para crear las salas de chat. Los chats se alojaban en servidores, siendo el más importante de habla hispana el famoso IRC Hispano. En él se alojaban diversas salas de chat con diversas temáticas, donde los usuarios charlaban sobre sus aficiones o temas de su interés.

Estas conversaciones eran dinámicas, puesto que el servidor no las almacenaba para poder ser consultadas después, y supusieron una de las vías para conocer a gente nueva que compartía intereses. Como parte negativa, el anonimato que proporcionan las salas de chat, las hacían idóneas para que usuarios malintencionados intentaran engañar a sus víctimas.

Los chats evolucionaron con la llegada de MSN Messenger, un programa de mensajería instantánea en el cual ya sólo se podía chatear con los contactos que se tuvieran agregados anteriormente. Esto añadía un primer filtro a la hora de conversar con gente, aunque también los usuarios malintencionados aprendieron a hacerse pasar por personas amigables, con el objetivo de ser añadidos al Messenger de la víctima, y una vez ganada su confianza, lanzaban su ataque.

Por otro lado, los grupos de News, siguen estado hoy en día activos. Son similares a foros, para los cuales es necesario acceder con un software específico. Estos "foros" han tenido siempre un marcado carácter profesional, y en grupos de news nacieron productos de software como Linux.

Estas aplicaciones, permiten comunicarse con personas de todas las partes del mundo, de una manera ordenada, pudiendo compartir contenido de diversa naturaleza, como estados, fotografías, vídeos, etc....

Generalmente, las redes sociales se dividen o bien por el uso, o bien por el contenido que se comparte. De tal manera que, por ejemplo, Instagram nació con una fuerte orientación por lo fotografía, aunque ha ido añadiendo funcionalidades con el paso del tiempo.

Facebook permite compartir todo tipo de contenido, y está orientado a ser una red más cerrada, pensada inicialmente para conectar a usuarios de la misma universidad.

Twitter en sus inicios sólo permitía compartir texto, y hasta un máximo de 140 caracteres, los mismos caracteres que se podían enviar en un SMS. Actualmente permite compartir actualizaciones de mayor longitud, además de compartir fotografías, vídeos, realizar encuestas, etc...

LinkedIn es una red social similar a Facebook en su funcionamiento, pero enfocada al ámbito profesional, por lo que los contenidos que se comparten están más orientados a un perfil profesional que al plano personal.

YouTube es una red social, en la cual sólo se comparten videos.

Google Plus, ha sido un intento de Google de crear una red social similar a Facebook, pero no ha tenido un gran éxito.

Como vemos, cada red social tiene un objetivo, y un público que tiene más interés en la manera en la que se comparte el contenido, por lo que cada una tiene elementos diferenciadores con las demás.

Además de estas redes sociales, que podríamos llamarlas "generalistas", existen todo tipo de redes sociales en torno a temas o comunidades concretas, o muy diferenciadas por el tipo de contenido que ofrecen, como, por ejemplo:

- Reddit
- Tumblr
- Flickr

Y un largo etcétera. Unidas a estas redes sociales, las aplicaciones de mensajería instantánea también tienen ya consideración de redes sociales, al permitir la interacción entre usuarios de diversas maneras, compartiendo estados, participando en grupos o canales, etc... Las más conocidas pertenecientes a esta categoría son WhatsApp y Telegram.

RIESGOS EN REDES SOCIALES

Las redes sociales, como ya hemos visto, son un instrumento fantástico para compartir experiencias, contenidos, vivencias, recuerdos, etc. con nuestros seres queridos, ya sean parientes, amigos, compañeros de clase, etc... Además, nos permiten participar en grupos de personas que tengan intereses semejantes, segmentado de esta manera el contenido, centrándose en la temática del mismo.

Todas estas herramientas han hecho que cambiemos nuestra manera de relacionarnos, de crear nuevas amistades o de compartir información.

Pero al igual que pueden suponer una gran ayuda, y un gran estímulo social, hay usuarios que hacen de las redes sociales usos no legítimos, aprovechando el anonimato de perfiles falsos, o cuentas hackeadas, con el objetivo de encontrar nuevas víctimas.

Pero no sólo los usuarios malintencionados suponen un peligro, nosotros mismos podemos cometer errores, principalmente debido al desconocimiento del uso de nuestros datos por parte de las redes sociales. Dar demasiada información, publicar imágenes o vídeos que nos puedan parecer "inocentes", pueden tener consecuencias en nuestras vidas en un futuro.

Por eso, queremos que uses las redes sociales, pero que lo hagas con responsabilidad y bajo la cautela necesaria, con el objetivo de que tengas la mejor experiencia posible y seas capaz de relacionarte con los demás de una manera saludable y productiva.

TU INFORMACIÓN ES SÓLO TUYA

Constantemente hemos estado repitiendo a lo largo de esta carpeta, que Internet no es más que un canal de transmisión de la información, y que las aplicaciones que utilizamos únicamente procesan la información que los usuarios les envían. Por lo tanto, cualquier información que publiques en una red social la publicas bajo tu propia responsabilidad.

Ser dueño de lo que publicamos es muy importante, porque como ya hemos comentado, en el momento en el que realizas una publicación en una red social, ya no sabes si alguien más la ha podido ver o guardar.

Esto puede suponer que esa fotografía comprometedora que has publicado por error, puede ya estar circulando por varios canales, y tú pensando que ya la habías eliminado.

CASO REAL

Fuente: ABC

https://www.abc.es/recreo/abci-roban-todas-pertenencias-publicar-foto-facebook-201608081854_noticia.html

En agosto de 2018, una joven pareja londinense publicó una foto en la cual anunciaban que iban a mudarse. La imagen no sólo fue motivo de agrado para sus seres queridos, sino también para unos ladrones, que aprovecharon para robarles el piso.

En concreto, los ladrones se hicieron pasar por los operarios del servicio de mudanzas para llevarse todas y cada una de las pertenencias de los jóvenes. Los objetos que les fueron robados estaban valorados en más de 12.000€, y a los ladrones les costó menos de una hora llevarse todo.

Cuando el camión no llegó a su destino, esta pareja se puso en contacto con la empresa de mudanzas, la cual les confirmó que habían sido víctimas de una estafa.

Como hemos podido comprobar, la información que para nosotros puede parecer inocente y llena de buenas intenciones, para algunas personas puede suponer una oportunidad de cometer delitos, o aprovecharse de ella para sus propios fines.

En muchas ocasiones, no somos conscientes de que una publicación aparentemente inocente, puede generarnos consecuencias en el futuro.

Actualmente, las empresas que realizan selección de personal para determinados puestos, consultan de manera previa a la entrevista de trabajo, los perfiles de redes sociales de los candidatos. En muchas ocasiones, se descartan candidatos porque el perfil de sus redes sociales no encaja con el que están buscando para cubrir la vacante.

Esto es un claro ejemplo de cómo puede afectar a nuestra vida, una publicación desafortunada en las redes sociales.

Aunque es posible que sea el caso menos dañino.

En otras ocasiones, cuando realizamos una publicación por error, no sabemos quién ha podido guardarla. Es posible que puedan utilizar un comentario, imagen o vídeo del cual nos hemos arrepentido de haber publicado, para generar burlas o bulos contra nosotros.

Fuente: 20 minutos

https://www.20minutos.es/noticia/2576965/0/emotiva-respuesta/chica-ridiculizada/internet-acne/

Ashley VanPevenage, es una chica estadounidense, que estaba realizando un vídeo sobre cómo cubrir el acné con maquillaje. Pero durante la sesión, sufrió una reacción alérgica al peróxido de benzoílo (usado para tratar el acné), por lo que su imagen durante el tratamiento era bastante "dramática".

Cuando subió las fotos de su tratamiento a Instagram, alguien la convirtió en un meme, a partir de ahí la imagen se hizo viral, y comenzaron a circular todo tipo de comentarios y bromas hirientes sobre su rostro en Internet.

Tras leer todos esos comentarios Ashley comentó posteriormente que "perdió la confianza en sí misma", y añadió que se dio cuenta de que las opiniones de la gente no le importan, y no deberían importar a nadie, refiriéndose a su aspecto.

En este caso, vemos como una imagen que posiblemente no tendría que haber salido del ámbito privado o del círculo más cercano, se ha hecho pública y convertida en viral. La privacidad de esta persona se ha visto comprometida, y ha supuesto que esta información circule por Internet de manera libre y sin control.

En otras circunstancias incluso, esto puede llevar a la creación de historias, o bulos que afecten de manera negativa a nuestra reputación y crear una imagen de nosotros que no se corresponde con la realidad, quedando además vinculada nuestra imagen a esa historia.

LA CONFUSIÓN ENTRE PRIVACIDAD Y ANONIMATO

Es importante, antes de profundizar de manera exhaustiva en el uso de las redes sociales, que sepamos distinguir entre la privacidad y el anonimato on-line.

Privacidad: *Parte más interior o profunda de la vida de una persona, que comprende sus sentimientos, vida familiar o relaciones de amistad.*

Anonimato: *Ocultar el nombre o la personalidad.*

Estos dos conceptos, como podemos ver, tienen cierta relación, pero es importante saber separarlos.

En Internet, ya desde sus inicios, se ha tendido siempre a guardar el anonimato. Usamos nicks o apodos para nuestras cuentas. Podemos cambiar nuestro nombre real por uno falso con el objetivo de que no se nos relacione directamente con la información que colgamos, o las acciones que realizamos en Internet.

La privacidad, como vemos, hace referencia a toda la información relativa a nuestra vida personal,

como pueden ser: aficiones, amistades, familiares, actividades que realizamos, la dirección de nuestra vivienda, la de nuestro instituto o colegio, nuestro trabajo, etc...

La facilidad que ofrece Internet para permanecer en el anonimato, muchas veces nos lleva a revelar información privada, que en algún momento nos puede perjudicar, pensando que somos anónimos, y nadie va a relacionar nuestros comentarios, fotografías o vídeos con nosotros.

Sin embargo, existe una práctica muy utilizada por usuarios malintencionados, para sacarnos del anonimato, el **doxing**.

DOXING

Práctica en Internet de investigación y publicación de información privada o con capacidad para identificar a una persona o una organización.

Esta práctica nace en el momento en el que es necesario obtener información sobre la persona que se esconde bajo un Nick o apodo, ya sea en un foro, en un chat, en un videojuego o en una red social, con el objetivo de identificarla y poder realizar sobre ella prácticas maliciosas.

En Internet existen multitud de herramientas para conseguir esta información, y se ha convertido prácticamente en una profesión que utilizan tanto los agentes de la autoridad como los atacantes para obtener información sobre una persona.

Gracias a estas herramientas, por ejemplo, se pueden encontrar correos electrónicos vinculados a cuentas de servicios en Internet, números de identificación, como D.N.I.´s, números de teléfono, direcciones, etc...

Es relativamente sencillo, por ejemplo, rastrear un nombre de usuario en Internet, y comprobar en qué páginas web existe este Nick. Gracias a estas herramientas, es posible rastrear la información existente sobre este apodo, hasta encontrar un servicio que vincule ese nombre a una dirección de correo.

Posteriormente, se realiza otra búsqueda con ese correo electrónico en portales o redes sociales, pudiendo localizar la cuenta a la que pertenece ese correo electrónico, averiguando de esta manera, más información sobre la persona en cuestión.

Una vez que se ha obtenido su nombre, siguen existiendo herramientas para realizar búsquedas en publicaciones oficiales, pudiendo llegar a obtener toda su información personal.

En muchas ocasiones, el doxing se realiza con la intención de obtener la identidad de una persona, con el objetivo de acosarla o de causarle un perjuicio. En otras ocasiones se realiza con la intención de identificar a los participantes de un vídeo o fotografía que se haya convertido en meme o viral, con el simple afán de sacar a la luz pública la identidad de las personas que están siendo objeto de mofa.

Es por este motivo, que cuando hacemos un uso intensivo de estos servicios, debemos ser muy conscientes de que el anonimato real no existe, y que nuestra privacidad sólo dependerá de lo bien que la podamos proteger.

COMO MANTENER LA PRIVACIDAD EN INTERNET

Actualmente existe mucha preocupación al respecto de la privacidad en Internet. Como usuarios nos damos cuenta de la importancia que tiene nuestra vida privada, y que hacerla pública puede hacernos mucho daño, tanto en el presente como en el futuro.

Desde las autoridades europeas se ha trabajado a lo largo del año 2018 en añadir medidas de protección a las empresas que utilizan nuestros datos, siendo este el primer paso de muchos que hay que dar para conseguir un marco legal que proteja nuestra información.

Sin embargo, tenemos que ser conscientes de que nuestra información es responsabilidad nuestra, y que en última instancia siempre seremos los responsables de haber hecho una foto, grabado un video o comentar en un foro, y que, si esta información por algún motivo llegara a hacerse viral, perderemos totalmente el control sobre ella, y nunca sabremos qué consecuencias puede tener en realidad.

Por ese motivo, es muy importante que sepamos mantener nuestra información personal, lo más privada posible, es decir, intentando no dar más información que la estrictamente necesaria.

Esto significa, que tenemos que tener mucha responsabilidad a la hora de publicar una foto, un vídeo, escribir un Tweet, publicar un estado en Facebook o escribir un comentario en un foro, ya que nos sabemos realmente cómo esa información puede afectarnos.

Si únicamente publicamos lo que realmente queremos publicar, y es información que no pertenece a nuestro ámbito más privado, no debemos más que seguir las recomendaciones que damos a continuación.

1º) Servicios de geolocalización

La geolocalización se conoce como los datos de posición respecto a un punto de la superficie terrestre. Esta posición generalmente se obtiene a través de los satélites del sistema GPS, y gracias al desarrollo de la tecnología prácticamente se ha conseguido eliminar los mapas en papel por innecesarios.

Los servicios de geolocalización son un añadido a muchas de las aplicaciones de nuestros smartphones, añadiendo funcionalidades nuevas, como recomendaciones de restaurantes, o construyendo un juego nuevo, como el Pokemon Go, caso que ya hemos visto.

Sin embargo, no sólo podemos geolocalizarnos por el sistema GPS, hoy en día se utilizan más medios para localizar la posición de un dispositivo. Sistemas como el 4G o las redes Wi-Fi, sirven para localizar nuestra posición, aunque no de manera tan exacta como el GPS (aproximadamente 200 metros, frente al GPS que tiene una precisión de 1 metro).

Es decir, nuestros smartphones conocen de manera constante la posición en la que nos encontramos, la dirección en la que nos movemos, los sitios que visitamos, el tiempo que estamos parados en un sitio, etc...

Pero también son capaces de identificar cuál es nuestra vivienda, simplemente sabiendo la posición en la que nos encontramos todas las noches, dónde está nuestro instituto o trabajo, ya que entramos y salimos todos los días a la misma hora, siguiendo más o menos todos los días la misma ruta.

Esta información, que es de utilidad para muchos servicios, en ocasiones no es importante o relevante para nosotros. Además, nunca sabremos con seguridad si una aplicación ilegitima está haciendo uso de esta información con otra finalidad más peligrosa.

Es, por tanto, muy importante, que los servicios de geolocalización de nuestros teléfonos estén siempre desactivamos, activándolos únicamente cuándo vayamos a hacer un uso efectivo de ellos. (Cuando vayamos a usar el GPS para encontrar una dirección, cuando queramos utilizar una aplicación para la que sea necesario, etc...)

APP DE LA LIGA

En junio de 2018, se hizo público que la aplicación oficial de La Liga activaba el micrófono del teléfono para saber si una persona estaba viendo un partido de fútbol. Con esta información, geolocalizan tu posición para saber si estás en un bar, y en ese caso, comprobar si ese establecimiento cuenta con la licencia necesaria para poder poner los partidos de La Liga en su televisión. De esta manera pueden detectar el fraude en establecimientos públicos no autorizados.

Por supuesto, en su aplicación informan de esta posibilidad, y hay que dar el consentimiento para que la aplicación pueda realizar esto, ya que, en este caso, la aplicación se ha programado con fines legítimos y por lo tanto no requieren intentar esconder esta funcionalidad.

La pregunta que nos hacemos es, ¿y si es una aplicación maliciosa?

En este caso debemos ser conscientes de la pérdida de privacidad que supone que una aplicación pueda espiar nuestras conversaciones y saber en qué lugar se están produciendo.

Metadatos

Cuando realizamos una fotografía, en el archivo que se crea no sólo se almacena la imagen en sí misma, sino que también se almacena otra información relativa a la cámara, a los parámetros que se han utilizado para realizar la fotografía, etc... Esta información se conoce como metadatos.

En caso de que la cámara tenga la posibilidad de geolocalizar el lugar en el que se ha realizado la fotografía, también la incluirá en estos metadatos, los cuales no se borran, aunque subamos la fotografía a un servicio en línea.

Esta información en muchos casos no es necesaria, y, sin embargo, da información sobre los lugares en los que estamos, o que hemos visitado. Además de localizarnos en el espacio, también lo hace en el tiempo, ya que la hora de realización de la fotografía también se graba en los metadatos.

Por lo tanto, alguien con los conocimientos y herramientas adecuados, puede saber exactamente dónde estábamos y a qué hora cuando hicimos la fotografía, por lo que podría llegar a identificarnos gracias a esta información.

2º) Uso de cuentas de correo temporales

En muchas ocasiones, necesitamos crear una cuenta para acceder a un servicio on-line, como por ejemplo un foro, ya bien sea porque queremos acceder a un

recurso que tienen en ese foro, o porque queremos consultar una información que necesitamos.

La mayoría de las veces, no volvemos a visitar esa página web nunca, e incluso es posible que, aunque hagamos un uso más o menos regular de ella, un día deje de estar disponible. ¿Qué pasa entonces con nuestros datos?

En ambos casos vemos que hemos tenido una pérdida de control de ellos, ya bien sea porque no volvemos a utiliza ese servicio, y se nos olvida que en él teníamos una cuenta y la hemos dejado sin borrar, o porque la página web ha dejado de funcionar, y no sabemos qué ha pasado con nuestra información.

Para estos casos, cuando vamos a utilizar un servicio del cual no sabemos si vamos a seguir utilizándolo en el futuro o no, podemos crear una cuenta de correo temporal.

Existen servicios web, como por ejemplo:
https://temp-mail.org
https://www.mohmal.com

que permiten crear una dirección de correo temporal, la cual pasado un tiempo dejará de existir, borrando todos los mensajes que ese correo tenga.

De esta manera, cuando creamos una cuenta en un servicio que nos solicita una dirección de correo electrónico, podemos utilizar una cuenta temporal sólo para el registro, evitando utilizar nuestra cuenta de correo.

Si en el futuro no volvemos a necesitar ese servicio, o deja de estar disponible, no deberemos preocuparnos por nuestra información, ya que esa cuenta de correo ya no existirá.

Como ventaja añadida, el uso de estas cuentas de correo evitará que en nuestra cuenta personal tengamos demasiado spam, ya que muchos de los servicios en los que nos damos de alta, utilizan nuestro correo electrónico para enviarnos publicidad, muchas veces de manera masiva.

3º) Diferentes cuentas, diferentes nicks

La tendencia, por norma general, es utilizar el mismo usuario y contraseña para todos los servicios en los que tenemos que crear una cuenta, de esta manera nos resulta más cómodo acordarnos de los datos de acceso.

Como ya hemos visto, el reutilizar contraseñas, nos pone en una situación de riesgo elevado si un usuario malintencionado la consigue, ya que comprometería todas las cuentas que tengan la misma contraseña.

Como medida adicional de seguridad, además de ayudar a proteger nuestra privacidad y anonimato, es muy recomendable utilizar diferentes nombres para cada cuenta. Y sobre todo, utilizar diferentes nombres de cuenta para nuestras redes sociales.

REDES SOCIALES

A lo largo de esta carpeta, hemos estado hablando sobre los riesgos existentes en Internet, y cómo pueden afectarnos de manera negativa a través de nuestros dispositivos. Hemos explicado qué son los virus informáticos y de qué manera afectan a nuestra privacidad, también hemos explicado cómo este software infecta a los diferentes dispositivos que tenemos, y la manera en la que los atacantes pueden utilizar nuestra información para causarnos daños o perjuicios.

También hemos hablado sobre la privacidad y el anonimato en Internet, conceptos importantes para tratar sobre el tema más importante de todos, las redes sociales.

Hemos hablado un poco sobre ellas, dando pinceladas pequeñas sobre su origen y su uso actual, a lo largo de este capítulo aprenderemos a hacer un uso responsable de las redes sociales.

Todas las redes sociales han nacido con la intención de ser una herramienta para conectar a personas. La forma en que se lleva a cabo de manera efectiva esta conexión o interacción entre personas, puede variar en función de la red social que estemos utilizando, enfocándose cada una hacia unos colectivos, intereses o grupos diferentes. Aunque todas tienen algo en común: nosotros somos su producto.

La información que compartimos, que comentamos, que recomendamos, los clics en "Me gusta", los retweets, los likes, etc... Todo esto es información y dicha información es utilizada por las redes sociales para crear perfiles de sus usuarios. Mediante éstos perfiles, se generan estudios de mercadotecnia que posteriormente pueden ser vendidos a terceros. Estos son los clientes de las redes sociales, son las empresas que pagan por anunciarse en ellas.

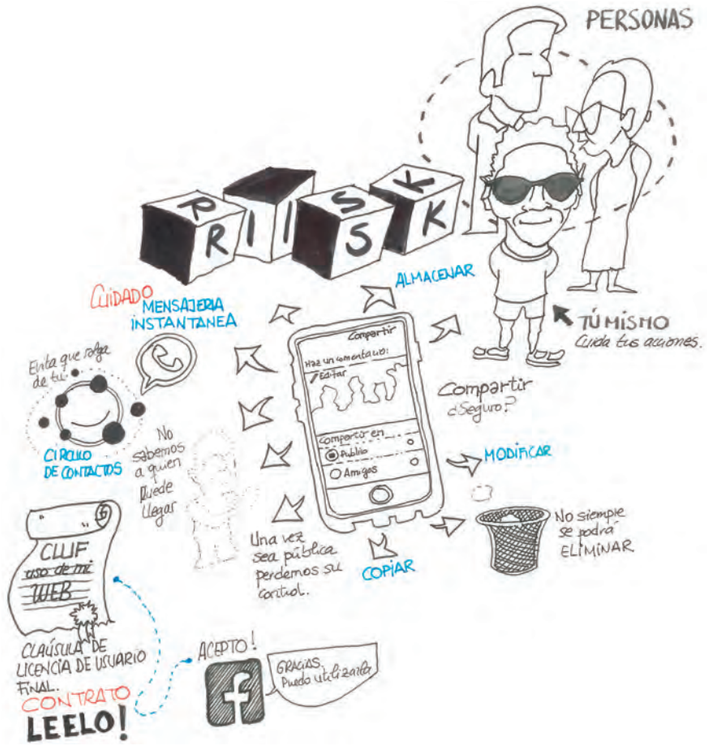
Por lo tanto, tenemos que ser conscientes, no sólo de todos los peligros que acechan en las redes sociales, sino que toda la información que les damos, la utilizan para sus fines como empresa, y con ningún otro objetivo que el de ganar dinero. Por lo tanto, tenemos que ser capaces, no sólo de utilizar las redes sociales como una herramienta que nos permite tener una vida social, profesional o personal más plena, sino como una herramienta que puede volverse en nuestra contra, sino somos nosotros los que ponemos las barreras y las medidas de seguridad apropiadas.

Un uso irresponsable de las redes sociales, no sólo puede tener consecuencias negativas en nuestra vida privada, como ya hemos visto, sino que además, puede tener otro tipo de consecuencias, desde laborales hasta penales. Esto significa que no sólo debemos hacer un uso responsable, sino que tenemos que estar alerta ante cualquier comportamiento que pueda ser sospechoso y que pueda suponer un riesgo para nosotros mismos o para terceras personas. Ante cualquier comportamiento sospechoso debemos ponerlo en conocimiento de manera inmediata a nuestros padres, profesores o las autoridades competentes.

De ninguna manera queremos que no se utilicen las redes sociales, lo que queremos es que todos y todas podamos utilizarlas de tal manera que sean una herramienta útil y que nos permitan tener relaciones sanas con nuestros amigos, compañeros, colegas y por supuesto, con nosotros mismos.

A lo largo de esta capítulo iremos recopilando una serie de consejos, ejemplos y además, pondremos el foco en las prácticas peligrosas que pueden poner en peligro nuestra vida privada, y en ocasiones extremas, nuestra seguridad física.

Por último, desgranaremos las redes sociales más populares para que podáis configurar los ajustes de seguridad y privacidad de la mejor manera posible, ayudándoos así a proteger tanto vuestra cuenta como vuestra privacidad.



LOS RIESGOS DE LAS REDES SOCIALES

En las redes sociales, el riesgo número uno son las personas. Al fin y al cabo no dejan de ser aplicaciones que sirven para conectar a personas. Esto, al igual que en la vida real, puede suponer un riesgo si somos demasiado confiados. Aunque en muchas ocasiones, no sólo son terceras personas las que pueden ponernos en riesgo, sino nosotros mismos con nuestras acciones.

Por eso, es importante conocer todos los riesgos asociados al uso de las redes sociales, y conocer más sobre ellos para detectarlos y evitarlos.

Uso ilegítimo de nuestras imágenes.

Anteriormente comentábamos que en el momento en el que subimos una foto a la "nube", ya bien sea publicándola en una red social o simplemente alojándola en nuestro almacenamiento privado, perdemos el control sobre esa imagen.

Concretamente, cuando colgamos una imagen en redes sociales, estamos haciendo pública esa fotografía o vídeo, y corremos el riesgo de que alguna persona, copie, almacene o modifique la imagen que hemos colgado.

Esto puede ponernos en un gran peligro de exposición y vulnerabilidad, ya que en el momento en el que esa imagen se haga pública, no podremos controlar por dónde se está difundiendo, ni a quién está llegando.

Si bien es cierto, aunque podemos solicitar a todas las páginas web dónde aparezca esta fotografía o vídeo que sea eliminado, no podremos controlar otras vías de difusión como aplicaciones de mensajería instantánea o foros de Internet privados.

Por lo tanto, para protegerse de este uso ilegítimo, debemos evitar subir imágenes o vídeos a entornos poco controlados. En el caso de que lo hagamos en nuestras redes sociales, estas imágenes debemos evitar que salgan de nuestro círculo de contactos.

En algunos casos, no debemos confundir el uso ilegitimo, con la cesión de los derechos de imagen.

El CLUF no es un BLUF.

CLUF, o Clausula de Licencia de Usuario Final, es un contrato que aceptamos en el momento de utilizar un servicio web, una aplicación o un programa. Generalmente los usuarios de estas aplicaciones, no solemos leer su contenido, y en ocasiones aceptamos clausulas las cuales, en caso de conocerlas, seguramente no las aceptaríamos.

En el caso de determinas redes sociales, cuando creamos nuestra cuenta, estamos aceptando la cesión de los derechos de imagen a la red social. Esto quiere decir, que si subimos una foto por ejemplo a Facebook, aunque nosotros seremos los dueños de la fotografía, la red social podrá utilizar esa imagen para lo que ella quiera, dentro de la propia plataforma.

De tal manera, que podemos aparecer en fotografías de anuncios o publicaciones de Facebook, las cuales llegan a muchísimas más personas. En algunas redes sociales, esto puede ser evitado, modificando y ajustando de manera correcta los parámetros de privacidad de nuestra cuenta.

CONOCE – RELACIÓNATE CON SEGURIDAD

Las redes sociales no sólo son utilizadas como un punto de unión entre personas, gracias a ellas también somos capaces de crear nuevas relaciones y conocer a gente nueva e interesante que comparta nuestros gustos y aficiones.

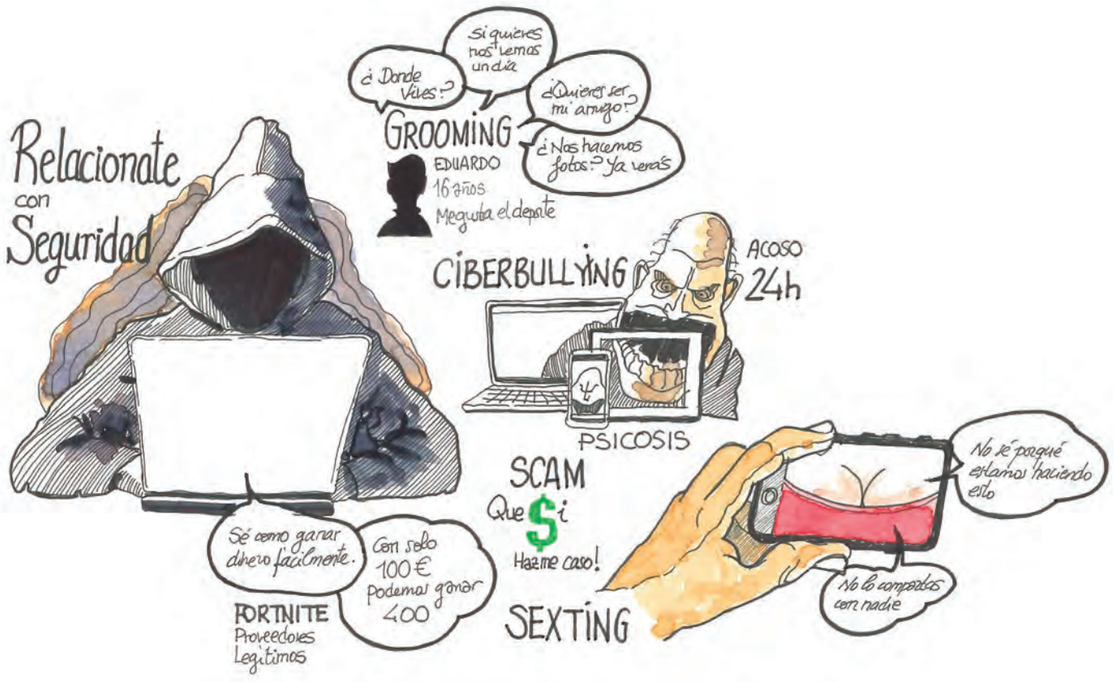
Para que estas nuevas relaciones sean sanas y constructivas, tenemos que tener en cuenta varios aspectos a la hora de llevarlas a cabo. A la hora de crear perfiles de redes sociales, en muchas ocasiones no se solicitan documentos que acrediten la identidad de la persona que se está registrando. Muchas veces, para crear un perfil en una red social basta con introducir una cuenta de correo electrónico válida, pero por otra parte para crear una cuenta de correo electrónico, simplemente no hace falta ningún dato, de donde se infiere que no hace falta ningún dato personal, ni ninguna corroboración de la identidad para crear un perfil en determinadas redes sociales.

El hecho de poder crear muchas cuentas en una misma red social, atrae a todas aquellas personas que quieren permanecer en el anonimato y realizar actividades ilícitas dentro de la red social. Muchas veces nos encontramos con perfiles con nombres falsos, fotos que no nos dicen nada acerca de quién es, ni proporcionan información sobre dónde viven o su edad.

Además, esta misma facilidad para crear perfiles propicia que existan perfiles falsos. Personas haciéndose pasar por quién no son, mintiendo acerca de su identidad. El motivo para registrarse con estos perfiles puede ir desde simplemente que una persona no quiera dar sus datos reales para participar en la red social, hasta personas que quieren engañarnos para hacernos daño.

Aunque las redes sociales ponen todo su empeño en detectar este tipo de perfiles, con el objetivo de eliminarlos e impedirles el acceso a la red, al final siempre encuentran la manera de conseguir acceso y continuar con sus actividades.

Dentro de las actividades que se realizan usando perfiles falsos, una de las más peligrosas es la que se conoce como grooming.



¿Qué es el grooming?

Esta actividad, realizada generalmente por delincuentes, consiste en la creación de perfiles falsos en las redes sociales creando identidades falsas, las cuales compartan datos con los de sus víctimas. El objetivo de estos usuarios generalmente es ganarse la confianza de sus víctimas, creando un vínculo emocional con ellas, con el fin de poder realizar acciones de abusos sexuales.

Para conseguirlo, esta práctica tiene varios procesos:

1º) El adulto intenta establecer lazos emocionales de amistad con el menor, para conseguirlo generalmente se hacen pasar por alguien de la misma edad, con los mismos intereses, creando para ello los perfiles falsos en redes sociales.

2º) Poco a poco, este adulto va consiguiendo información personal del menor, incluyendo los datos de contacto.

3º) Utilizando tácticas de seducción, provocación y engaño el adulto consigue finalmente que la víctima le envíe imágenes con alto contenido sexual, o bien cualquier otro tipo de información que pueda resultar muy comprometedora.

4º) Una vez que el adulto ha conseguido estas imágenes o información, comienza la fase de extorsión durante la cual, gracias a toda la información que ha ido consiguiendo del menor le solicita que le siga enviando imágenes o vídeos, incluso llegándole a pedir encuentros físicos para abusar sexualmente de él.

Cuando alguien es víctima de este tipo de delincuentes, es muy difícil conseguir que acuda a las autoridades o hable con sus padres, ya que el miedo que el delincuente ha provocado en la víctima a hacer públicas todas las imágenes o información que ha ido recopilando, sitúa a la víctima en una situación de vulnerabilidad y bloqueo muy difícil de superar.

Como siempre, para evitar caer en este tipo de engaños, la herramienta número uno es la prevención, por eso es muy importante seguir unas normas básicas cuando tenemos contacto con desconocidos a través de Internet.

La regla de oro es que cuando estemos hablando con personas que no conocemos en Internet, no desvelemos ningún dato personal. Los delincuentes nos pedirán números de teléfono, dirección, etc... Todo con el fin de que cuando llegue el momento, puedan ejercer toda su presión y acoso para evitar que la víctima denuncie lo sucedido.

Debemos ser muy cautos a la hora de aceptar peticiones de amistad de personas que no conocemos.

En las redes sociales, tenemos que tener en cuenta que muchas, veces en el momento en el que agregamos a una persona a nuestro círculo de amistades consigue tener acceso a mucha información personal sobre nosotros. Ya puede mirar todas nuestras publicaciones, consultar toda la información que hemos colgado, hacer un seguimiento de los comentarios que publicamos, los grupos a los que pertenecemos, las personas a las que seguimos. Incluso tiene acceso a más información sobre todos nuestros contactos, pudiendo de esta manera llegar a más personas.

En muchas ocasiones, no van de manera directa a por la víctima, sino que primero se van introduciendo a través de su círculo de amistades, para que llegado el momento de contactar por primera vez con ella, ya tiene un trasfondo o recorrido y una coartada sólida en la que fundamentar el acceso directo a la víctima.

Por lo tanto, siempre es mejor tener un contacto previo utilizando las herramientas que las redes sociales ponen a nuestra disposición antes de aceptar una solicitud de amistad.

Preguntar directamente quién es la persona que nos ha mandado la invitación, o por qué lo ha hecho, generalmente disuaden al atacante de seguir en su empeño. En el caso de que anteriormente la persona ya haya entablado relación con las personas más cercanas a nosotros, también podemos preguntarles directamente a ellas, para obtener más información acerca de cómo lo han conocido, o cómo ha contactado con ellos.

Tener claro los filtros que ponemos a la hora de incluir a más personas en nuestras redes sociales es muy importante cuando queremos evitar prácticas de este tipo. Muchos tipos de engaño comienzan por solicitudes de amistad que aparentan ser inocentes, por eso no aceptes invitaciones de personas que no conozcas o de perfiles que te parezcan sospechosos. Ante la duda, di siempre NO.

CIBERBULLYING

Aunque todos estamos muy concienciados de los peligros del bullying y de cómo esta práctica daña a las personas que la sufren, con la llegada de las redes sociales y su popularización, el acoso que anteriormente se reducía a espacios físicos, ahora trasciende estas fronteras volviéndose muchísimo más peligroso y constante en el tiempo.

El hecho de que podamos acceder a las redes sociales desde cualquier dispositivo y desde cualquier lugar, hace que las personas que realizan el ciberacoso lo hagan a todas horas y desde cualquier parte.

De esta manera, la víctima no tiene descanso ni en casa ni en clase ni en la biblioteca ni en la calle.

Además el daño se produce en cualquier momento por la mañana, por la noche, los fines de semana... A todas horas le están apareciendo notificaciones, de todas las redes sociales, agravando el problema y haciendo que la víctima no tenga descanso, ni margen para reaccionar. Esto puede provocar una situación de psicosis ya que la víctima nunca puede predecir en qué momento recibirá el siguiente ataque, por lo que se genera una situación de tensión constante. Además, el ciberbullying tiene una característica que lo hace aún más peligroso que el bullying, y no es otro que la naturaleza de Internet.

Internet siempre ha intentado favorecer el intercambio de información de manera abierta y libre, y esta naturaleza hace que las prácticas de ciberbullying se vuelvan mucho más peligrosas, debido al fenómeno de la viralización.

Debido a esto, en muchas ocasiones son otras personas las que se unen al acoso que están realizando unos pocos, aprovechando de nuevo, el anonimato y la sensación de impunidad que proporciona Internet. Por culpa de todo esto, la víctima ve como otras muchas personas, a las que ni siquiera conoce de nada se suman al acoso, publicando datos personales, de contacto, fotografías, vídeos, y cualquier material o información que pueda generar más daño y seguir alimentando la bola de la mofa y del acoso.

Cuando se llega a este punto es muy difícil pararlo, ya que ha escapado a los límites que puede controlar una persona. Recibir llamadas o mensajes a todas horas de números de completos desconocidos, ser mencionado en redes sociales por cientos, e incluso en ocasiones, miles de personas de forma constante sin un momento de descanso genera una situación que deja a la persona totalmente indefensa ante semejante ataque.

Es por esto, que es muy importante mantener una actitud vigilante ante estas prácticas, y denunciarlas en cuanto se vean, ya que los problemas que se pueden derivar son muy graves.

Por supuesto, si en algún momento conoces o sabes de alguna persona que esté pasando por esta situación, no dudes ni un momento en comunicarlo. Padres, profesores o autoridades tienen la competencia y las herramientas necesarias para denunciar estos hechos y poner freno a estas prácticas.

Y si en algún momento tienes la sensación de que puedes estar siendo víctima de una práctica de este tipo, no dudes en utilizar las herramientas que ponen a disposición las redes sociales, para bloquear usuarios y eliminarlos de tus contactos. Es lo mejor ante una situación de este tipo.

SEXTING

Como ya hemos estado mencionando a lo largo de todos estos capítulos, las redes sociales e Internet, han cambiado la manera en la que nos relacionamos con los demás.

Por supuesto, dentro de las relaciones humanas, una de las más importantes es la relación afectiva. Estas relaciones han ido cambiando a lo largo del desarrollo de Internet, llegando en la actualidad a un alto grado de interacción.

De esta manera de relacionarse, aparece la práctica conocida como sexting, la cual consiste en enviar, utilizando la facilidad de uso que proporcionan las nuevas tecnologías, contenido sexual altamente explícito a través de Internet a nuestra pareja.

Esta práctica, puede tener consecuencias negativas si no actuamos con responsabilidad. Tanto el emisor como el receptor de estos vídeos o fotografías, tienen que ser conscientes de que estas imágenes que se están compartiendo, forman parte del ámbito privado, y que están siendo enviadas confiando en la lealtad y responsabilidad de la otra persona.

Hay que ser muy críticos con aquellas personas que presuman en público, de las imágenes que han recibido aunque sea de parte de sus parejas, ya que lo han hecho confiando en que no iban a ser expuestas a terceros.

Además de esto, si las imágenes llegan a aparecer en redes sociales, no sólo estamos traicionando la confianza de la persona que las ha enviado, sino que además, podemos estar incurriendo en una práctica que puede ser delictiva. Hay que tener presente que compartir imágenes sin consentimiento expreso de la persona es un delito.

En ciertas ocasiones, también hemos podido ver que la persona de la que se han publicado esas imágenes, ha sufrido posteriormente ciberbulling, siendo todavía mayor el agravio que se le ha causado.

Por todos estos motivos, es muy importante que sepamos mantener la intimidad de las personas que han confiado en nosotros, y que si una imagen o vídeo ha sido compartido a través de una vía privada, debe permanecer en ese ámbito.

NO LE DES BOLA AL BULO

Una de las prácticas que más tiempo llevan realizándose, pero que más difícil es de ponerle freno, son los bulos en Internet. Si bien los bulos, y las noticias falsas son tan antiguas como la propia escritura, hoy en día con los medios de comunicación modernos en cuestión de horas un bulo puede haber llegado a millones de personas.

Internet como medio de comunicación tiene, además de la facilidad de uso, acceso y disponibilidad, una característica que lo hace completamente único: la inmediatez. Podemos publicar una noticia, la cual un segundo más tarde está siendo consultada por una persona situada en la otra punta del mundo. Esta ventaja a la hora de compartir información y vivir en la época en la que mejor informados estamos, también es aprovechada por ciertas personas grupos e incluso países para intentar colar noticias falsas. Las noticias falsas y los bulos pueden tener una gran diversidad de objetivos que pueden ir desde llamar la atención, conseguir visitas para una página web o un perfil en una determinada red social, simplemente por hacer la gracia o en ocasiones pueden tener como objetivo influir en la opinión pública o minar la credibilidad de otras fuentes de información.

Estas noticias falsas, sin embargo, también pueden suponer un riesgo.

En esta ocasión te invitamos a que descubras cuáles de los siguientes tres titulares es el real:

Titular A: TRIATLETAS CONTRATAN UN SEGURO POR VALOR DE UN MILLÓN DE LIBRAS EN CASO DE QUE SEAN HERIDOS POR EL MONSTRUO DEL LAGO NESS.

Titular B: UN AVIADOR BATE EL RÉCORD DEL MUNDO DE VUELO SIN ESCALAS CON UN AVIÓN FABRICADO POR ÉL MISMO.

Titular C: CHINA APROBARÁ EL AÑO QUE VIENE UN IMPUESTO AL "AIRE". CIUDADANOS Y TURISTAS DEBERÁN PAGAR UNA CANTIDAD POR EL AIRE CONSUMIDO.

La facilidad con la que se puede manipular la opinión pública actualmente es muy grande. Esto es debido a la inmediatez con la que se reproduce la información gracias a Internet, y en algunos casos la dificultad de contrastar las fuentes, esto hace que constantemente se publiquen noticias que no corresponden con la realidad.

Actualmente, la red social dónde más noticias falsas se difunden es Twitter, debido a su naturaleza inmediata y abierta, seguida muy de cerca por las aplicaciones de mensajería instantánea.

Como usuarios y consumidores de información, debemos mantener siempre una actitud crítica ante todo tipo de informaciones, e intentar poner en duda todo aquello que nos parezca sospechoso y demasiado raro para ser verdad.

Debemos consultar siempre fuentes fiables y reputadas para contrastar las noticias que nos lleguen, ya que de manera general, los medios de comunicación más tradicionales intentan mantener el rigor informativo y la seriedad.

Como usuarios, debemos mantener una actitud responsable ante los bulos y noticias falsas, intentando no seguir con su difusión y haciendo aclaraciones en caso de que sepamos que una noticia no es cierta.

Por supuesto, no nunca debemos fomentar la creación ni la difusión de noticias falsas o bulos, pero sobre todo tenemos que prestar especial atención cuando se trate de entornos cercanos, ya que estas falsedades pueden generar situaciones de alarma o generar algún tipo de perjuicio para otras personas.

Si todos colaboramos evitando difundir este tipo de mentiras, obtendremos un beneficio común, el de estar informados de manera verídica y rigurosa.

OTROS TIPOS DE ENGAÑOS (SCAM)

En las redes sociales, las prácticas de riesgo no se limitan a actos como los que hemos estado describiendo hasta ahora. En la actualidad, los usuarios malintencionados o delincuentes, han encontrado otras maneras para obtener beneficios, aprovechándose de la confianza de las demás personas.

En los últimos tiempos estamos viendo casos de personas que denuncian haber sido estafadas por otras personas, ya bien sea porque les han pedido dinero, favores o han ofertado trabajos que finalmente terminan siendo una estafa.

Para evitar este tipo de engaños, debemos actuar de manera responsable en las redes sociales, de igual manera que actuamos en la vida real.

Si caminando por la calle, un día una persona desconocida te ofrece ganar mucho dinero a cambio de únicamente diez euros, ¿qué le contestarías? Obviamente te generaría muchas dudas, sabríamos que hay gato encerrado y que lo más probable es que si le damos el dinero que nos pide, no volvamos a ver nunca ni a esa persona ni a nuestro dinero.

En Internet hay que actuar de igual manera.

Pongamos como ejemplo, que nos llega una solicitud de amistad de una persona desconocida. Por curiosidad la aceptamos y le preguntamos quién es.

Esta persona, que seguramente nos habrá estado espiando, y sabrá que tenemos algún punto débil por ejemplo, nos dirá que tiene un sistema para ganar todas las partidas a nuestro juego favorito, o que conoce a una persona que nos puede hacer ganar un dinero extra, o conseguir tarjetas prepago más baratas.

Si entramos en su juego, poco a poco nos intentará convencer de que está diciendo la verdad, llegando incluso a enviarnos imágenes que refuercen sus argumentos. Estas imágenes seguramente serán falsas o estarán manipuladas.

Una vez que estemos convencidos, nos solicitará que le enviemos una cantidad de dinero.

Si lo hacemos, una vez que esta persona tenga el dinero, veremos como de repente, desaparece. Se ha completado la estafa.

Aprovechando el tirón que tienen los juegos para móviles, videoconsolas, etc... Estamos viendo como las estafas empiezan a dirigirse contra usuarios de estas aplicaciones.

El último caso conocido tiene que ver con el famoso videojuego Fortnite, el cual en el momento de redactar esta carpeta, aún no ha sido publicado para dispositivos Android.

Los delincuentes han visto el tirón que tiene este juego, y han publicado tanto en Play Store como en páginas web, aplicaciones que simulan ser el juego real, o la posibilidad de tenerlo antes que los demás.

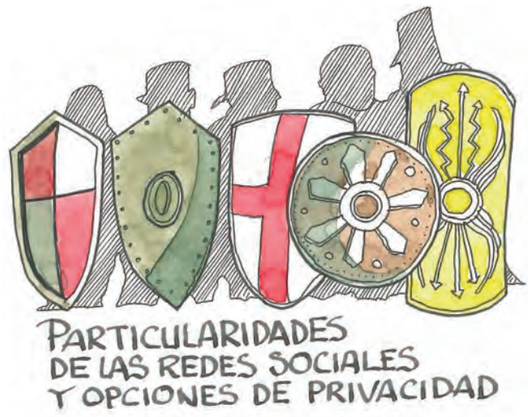
Una vez que la víctima del engañó entra en dicha página web o descarga la aplicación, se le solicita un número de teléfono para poder acceder al juego.

Por supuesto, una vez introducido el número seguiremos sin poder acceder al juego, sin embargo, nos habremos suscrito a un servicio de mensajería Premium teniendo que pagar por cada SMS que nos envíen. Y como ya estarás imaginando, no tendrás acceso al juego.

Instalando aplicaciones que prometen funcionalidades o servicios que aún no están disponibles, o que complementan de manera "maravillosa" a una aplicación famosa, generalmente no sólo no van a cumplir lo que prometen sino que además, estaremos instalando algún tipo de software malicioso que puede generarnos problemas. Pudiendo ser desde software que nos muestre publicidad de manera indiscriminada, hasta malware para controlar y acceder a nuestro teléfono u ordenador de manera remota.

Por eso, sólo debemos instalar aplicaciones que sean legítimas y que vengan de proveedores confirmados por las tienes de aplicaciones, intentando evitar instalarlas desde otras fuentes.

PARTICULARIDADES DE LAS REDES SOCIALES Y OPCIONES DE PRIVACIDAD



Hemos estado viendo cuáles son las prácticas más peligrosas en las redes sociales, y de qué manera nos pueden afectar de manera negativa, tanto a nosotros mismos como a nuestro entorno cercano. Estas actividades maliciosas son independientes de la red social que estemos utilizando, ya que nos las podemos encontrar en todas ellas, por eso se hace necesario profundizar un poco en cada una de las redes sociales existentes actualmente, y de qué manera podemos usarlas para protegernos a nosotros y a los demás.

A lo largo de este capítulo, iremos describiendo las particularidades de cada red social respecto de la privacidad del usuario, así como las configuraciones que nos ofrecen para proteger nuestra información y nuestras publicaciones.

Las herramientas que ponen a nuestra disposición, como usuarios de estas redes, son cada día más completas, ya que tanto a raíz de diversos escándalos que han surgido en los últimos tiempos sobre filtraciones de datos personales a terceros y los nuevos cambios normativos referentes a protección de datos personales, han hecho que las redes sociales tengan como una de sus prioridades la protección de esta información.

Aunque generalmente desde las redes sociales que utilizamos, no suelen informarnos- de manera activa sobre estas posibilidades, la configuración correcta de las opciones de privacidad y seguridad nos ofrece la posibilidad de conseguir que nuestros perfiles de redes sociales estén protegidos de miradas "indiscretas" o poder evitar ser etiquetados en publicaciones de otras personas sin nuestro consentimiento expreso.

Además, en este capítulo también veremos alguna de las técnicas que utilizan los usuarios malintencionados para obtener información sobre nosotros, y qué medidas de protección podemos utilizar para evitar ser su objetivo.

"LA RED SOCIAL" – FACEBOOK

Esta red social, aunque ahora esté cayendo en desuso paulatinamente, fue la que dio el pistoletazo de salida al boom de las redes sociales. Utilizada actualmente por más de dos mil millones de personas en el mundo, es la red social que más usuarios tiene.

Además, en los últimos tiempos, esta red social se ha visto salpicada por casos de filtración de información, y la utilización de esta información con fines políticos.

CAMBRIDGE ANALYTICA

En marzo de 2018, varios periódicos denunciaron que la empresa Cambridge Analytica había utilizado datos recopilados por Facebook para realizar las campañas electorales del Bretix y de las elecciones presidenciales de Estados Unidos de 2016.

Los datos recopilados de aproximadamente 50 millones de usuarios de Facebook, permitió crear perfiles sobre las inquietudes, deseos y necesidades de estas personas, para poder dirigir la publicidad hacía el resto de una manera efectiva y eficaz.

Posteriormente la empresa tuvo que cerrar por el escándalo, y Facebook perdió 37 mil millones de dólares en un día debido a este escándalo.

Por supuesto, los que más perdieron fueron los usuarios de la red social los cuales se han sentido desprotegidos y a merced de las empresas que quieran utilizar sus datos personales con el fin de obtener beneficios.

Facebook, debido a su posición dominante en el mercado de las redes sociales, siempre ha estado bajo sospecha en todo lo relativo a seguridad y privacidad, es por este motivo que siempre han intentado tener una política de seguridad respetuosa con el usuario ofreciéndole muchas opciones para mejorar su privacidad y la seguridad de su cuenta.

Generalmente, como en todas las redes sociales, estas opciones no están activadas en el momento en el que creamos la cuenta y debemos activarlas por nosotros mismos.

CONSEJOS PARA FACEBOOK:

Dentro de las muchas opciones que se pueden establecer en Facebook, recomendamos establecer las siguientes opciones de privacidad como medidas básicas de protección. Por supuesto, contra más restricciones impongas a tu perfil más protegida tendrás tu privacidad.

Para acceder a las opciones de privacidad, debemos acceder con nuestra cuenta a Configuración > Privacidad:

- **Visibilidad de las publicaciones:** Estas opciones afectan a quién puede ver las publicaciones que realices en tu biografía de Facebook.

  - Público: Todas las personas de la red social podrán ver las publicaciones que hagas, estén o no en tu lista de amigos. Esta opción no se recomienda en ningún caso, especialmente para perfiles con fines personales.

  - Amigos: Sólo las personas dentro de tu lista de amigos podrán ver las publicaciones. En este caso tu privacidad estará relativamente a salvo siempre y cuando sepas a quien estás aceptando como amigo.

  - Amigos excepto...: Esta opción permite que las personas de nuestra lista de amigos que decidamos no vean nuestras publicaciones.

- **Peticiones de amistad:** Establecer quién puede enviarte peticiones de amistad es muy útil para filtrarlas. Recomendamos establecerlo en Amigos de amigos.

- **Ver tu lista de amigos:** Lo recomendado es establecerlo en Solo yo.

- **Búsqueda con correo electrónico/número de teléfono:** Esta opción hay que establecerla en Amigos, de esta manera no se podrá enlazar nuestro perfil de Facebook con nuestra cuenta de correo. Esta acción es muy importante para mantener protegida nuestra privacidad.

- **Motores de búsqueda fuera de Facebook:** Esta opción es muy importante establecerla en NO. Si no se hace así, buscadores como Google tendrán información sobre nuestro perfil de Facebook, facilitando la búsqueda de personas a través de este buscador. Es una medida contra el Doxing.

En Biografía y etiquetado, tendremos opciones para controlar quién nos puede etiquetar en publicaciones y en qué circunstancias. Establecer estas opciones de manera correcta es importante para evitar ser etiquetados o incluidos en publicaciones de otras personas que no sean de nuestro agrado.

- **Publicaciones de otros en nuestra biografía:** Lo recomendable es tenerlo configurado en Amigos, de esta manera, sólo nuestra red podrá ver las publicaciones que otros hacen en nuestra biografía.

- **Revisar las publicaciones en las que se te ha etiquetado:** Esta opción nos permite revisar cualquier publicación en la que se nos incluya de alguna manera. Puede ser una etiqueta en una foto, una mención en un comentario, etc... Para que esta etiqueta se publique en nuestra biografía, previamente deberemos dar consentimiento expreso.

- **Revisar las etiquetas que otras personas añaden en tus publicaciones:** En Facebook, cuando publicamos por ejemplo, una fotografía, es posible que otras personas añadan a otras personas etiquetándolas. Gracias a esta opción, podremos revisar todas las etiquetas que se añadan a nuestras publicaciones antes de publicarlas. Hay que tener en cuenta que cuando se aprueba una etiqueta, la persona etiquetada y sus amigos podrán ver tu publicación.

Dentro de las opciones de Privacidad de Facebook, tenemos una opción para comprobar cómo se ve nuestro perfil, tanto de manera pública, como si fuéramos una persona en concreto. De esta manera, podemos ir ajustando los parámetros de privacidad e ir comprobando de qué manera está afectando a los contenidos que ven las demás personas.

HERRAMIENTAS PARA PROTEGER TU CUENTA

Al igual que Facebook ofrece opciones para proteger tu privacidad de las miradas indiscretas de los demás usuarios, también ofrece opciones para proteger el acceso a tu cuenta. Estos ajustes son accesibles desde el apartado Seguridad e inicio de sesión, dentro de la configuración de la cuenta.

Desde aquí podrás cambiar tu contraseña de acceso, lo cual es recomendable hacer cada cierto tiempo (tres o cuatro meses es lo ideal) además de poder establecer una serie de opciones que añaden más seguridad a la cuenta:

- **Autenticación en dos pasos:** Activar esta modalidad de acceso proporciona una seguridad extra a la hora de acceder a tu cuenta, ya que además de la contraseña, cuando inicies sesión, Facebook solicitará que introduzcas un código que se enviará a tu teléfono. De esta manera,

aunque alguien conociera tu contraseña, todavía necesitaría tener acceso a tu teléfono para poder acceder a tu cuenta.

- **Recibir alertas sobre inicios de sesión:** Gracias a esta opción, cada vez que se inicie sesión desde un dispositivo no usado de manera habitual, recibirás un correo electrónico informándote de ello. De esta manera, podrás saber si alguien ha accedido o ha intentado acceder a tu cuenta desde algún lugar, dándote tiempo para tomar acciones para protegerte.

Uno de los apartados más importantes es el que nos muestra los dispositivos desde los que se haya iniciado sesión, pudiendo ver una lista completa de ellos. Esto nos permite saber si nuestra cuenta ha sido abierta o accedida desde un dispositivo desconocido. Ten en cuenta, que debido a la configuración de tu proveedor de Internet, es posible que la ubicación que aparezca en este apartado no se corresponda tu ubicación real.

HAN ENTRADO EN MI CUENTA ¿QUÉ HAGO?

Como hemos visto, los ataques son cada vez más sofisticados y peligrosos. El hecho de que en algún momento alguien consiga acceder a una de nuestras cuentas es algo con lo que tenemos que contar, y debemos tener un *plan de acción* para reaccionar a tiempo y de manera que se produzca el menor daño posible.

Cuando descubramos, o **sospechemos** que una de nuestras cuentas on-line ha sido vulnerada, lo primero que debemos hacer es **CAMBIAR TODAS LAS CONTRASEÑAS.** Tenemos que tener claro que si han conseguido acceso a una de nuestras cuentas, pueden tener información para acceder a las demás, por lo tanto, es muy importante cambiar las contraseñas de manera inmediata.

Hay que tener especial atención con las contraseñas de nuestras cuentas de correo electrónico, ya que se utilizan para cambiar las contraseñas de los demás servicios. Cuando solicitamos el cambio de contraseña de una cuenta, por ejemplo de Facebook, el proceso habitual es que antes de hacer el cambio se envía un correo electrónico para confirmar el cambio de contraseña. Por lo tanto, si perdemos el acceso a la cuenta de correo, es muy posible que perdamos el acceso a nuestras demás cuentas.

Una vez que hayamos cambiado todas las contraseñas de los servicios que utilizamos de manera habitual, el siguiente paso es evitar que nos roben la contraseña de nuevo. Como en este punto no sabremos de qué manera la han obtenido, de nuevo la mejor práctica es actuar como si todos nuestros dispositivos hubieran sido atacados.

Siguiendo esta línea, debemos:

- Hacer copia de seguridad de toda la información almacenada en nuestro teléfono, ordenador, Tablet, etc...
- Restaurar al estado de fábrica todos los dispositivos desde los que hayamos accedido a nuestras cuentas
- Volver a copiar la información que hemos guardado en el punto primero.

De esta manera, en caso de que hubiéramos sido víctimas de un virus, estaremos casi seguros de que no nos vuelven a robar las contraseñas.

En el caso de que una de las cuentas que se haya visto comprometida, sea una cuenta bancaria o de algún monedero electrónico como PayPal, y nos hayan robado dinero, también tendremos que poner una denuncia ante los cuerpos y fuerzas de seguridad del estado.

Otras opciones de privacidad en Facebook

Hemos visto las opciones de privacidad más importantes que ayudan a mantener nuestra información a salvo de miradas "indiscretas". Además de todas estas, existen varias opciones que nos ayudan a mantener a salvo nuestra privacidad:

- **Historial de ubicaciones:** Es importante, como hemos visto en apartados anteriores, desactivar la geolocalización siempre que sea posible y que no sea realmente necesario. De esta forma evitamos fugas de información. En Facebook podemos desactivar la geolocalización de forma que no se almacene información sobre los sitios a los que vamos o visitamos.

- **Bloqueo:** Es importante saber que existe la opción de bloquear a una persona en Facebook, de esta manera, no podrá acceder a nuestro perfil ni ponerse en contacto con nosotros a través de la red social ni a través de la aplicación de mensajería instantánea de Facebook, Messenger.

caciones tienen una característica muy particular, son eliminadas 24 horas después de su publicación, sin dejar rastro ni en nuestro perfil ni en el de las personas que lo han visto, compartido o interactuado con él.

Esta sensación de volatilidad, confiere a estas publicaciones un riesgo adicional, podemos confiarnos demasiado a la hora de publicar contenido. Sabiendo que, como máximo 24 horas después de su publicación, este contenido va a ser eliminado, podemos publicar imágenes o vídeos que en otras circunstancias no subiríamos a las redes.

INSTAGRAM – EL FACEBOOK DE LAS IMÁGENES

Esta red social basada, empezó basándose íntegramente en la fotografía, evitando otro tipo de contenido. De esta manera supo destacarse sobre el resto, añadiendo los ya famosos *filtros de Instagram* y empezando a conseguir gran popularidad.

Tras permitir la publicación de vídeos, y sobre todo con las famosas "Stories", es una red social que está en alza y además tiene particularidades que la hacen especialmente sensible con nuestros datos privados. Es por este motivo que tenemos que prestar más atención a la hora de las publicaciones que realizamos en esta red social y ser más prudentes y precavidos.

-Stories, una bonita historia que puede acabar mal

El concepto de las stories de Instagram no es nuevo, Snapchat ya lo introdujo hace tiempo. Estas publicaciones tienen una característica muy particular, son eliminadas 24 horas después de su publicación, sin dejar rastro ni en nuestro perfil ni en el de las personas que lo han visto, compartido o interactuado con él.

Esta sensación de volatilidad, confiere a estas publicaciones un riesgo adicional, podemos confiarnos demasiado a la hora de publicar contenido. Sabiendo que, como máximo 24 horas después de su publicación, este contenido va a ser eliminado, podemos publicar imágenes o vídeos que en otras circunstancias no subiríamos a las redes.

Sin embargo, aunque la red social ha anunciado que va a tomar medidas al respecto de esto, durante el tiempo que la publicación que hemos hecho está en funcionamiento, nada impide que otro usuario obtenga una copia de la misma. De esta manera puede empezar a circular una imagen o vídeo nuestro por la red, el cuál pensábamos que había sido eliminado.

Como ves, esta posibilidad refuerza la idea de que cuando publicamos información en Internet, inmediatamente perdemos el control sobre la misma, pudiendo caer en manos de personas que traten esa información con fines malintencionados.

Por otro lado, Instagram ha pretendido ser una red social abierta, similar al concepto de Twitter. Esto quiere decir que si no lo indicamos de manera expresa, todas las publicaciones que hagamos en esta red social, podrán ser vistas por cualquier persona, tenga o no una cuenta activa en Instagram.

El hecho de que cualquier información que publiquemos sea accesible desde cualquier parte, por cualquier persona y en cualquier momento, hace que tengamos que ser muy responsables a la hora de publicar contenido en esta red social ya que nunca sabremos quién puede estar mirando, ni las intenciones que tiene con nuestras publicaciones.

En esta red social también tienen mucha relevancia los perfiles falsos. Esto se debe a que Instagram no solicita información personal adicional para comprobar la veracidad de los datos e impedir que una misma persona tenga dos o más cuentas. De esta manera, se puede generar una red entera de perfiles falsos que apoyen a las cuentas utilizadas para realizar los engaños, acosos y demás actividades ilícitas en la red.

Es por lo tanto muy importante concienciarse al respecto de que en esta red social, nosotros mismos somos los responsables de mantener a salvo nuestra privacidad y que debemos más que nunca, mantener una actitud vigilante y desconfiada ante perfiles que no conozcamos y que nos puedan parecer sospechosos.

Aunque Facebook hace tiempo que adquirió Instagram, los avances en la protección de la privacidad que ha mostrado Facebook en este tiempo no se han trasladado a esta otra red social. Aun así, sigue habiendo opciones de configuración que nos permiten añadir protección extra a nuestra cuenta tanto desde el punto de vista de la privacidad como de la seguridad.

-Privacidad de la cuenta:

Las opciones de privacidad de la cuenta, son accesibles tanto accediendo a la página web de Instagram en un navegador web, como a través de la aplicación de móviles. Aunque hay varias:

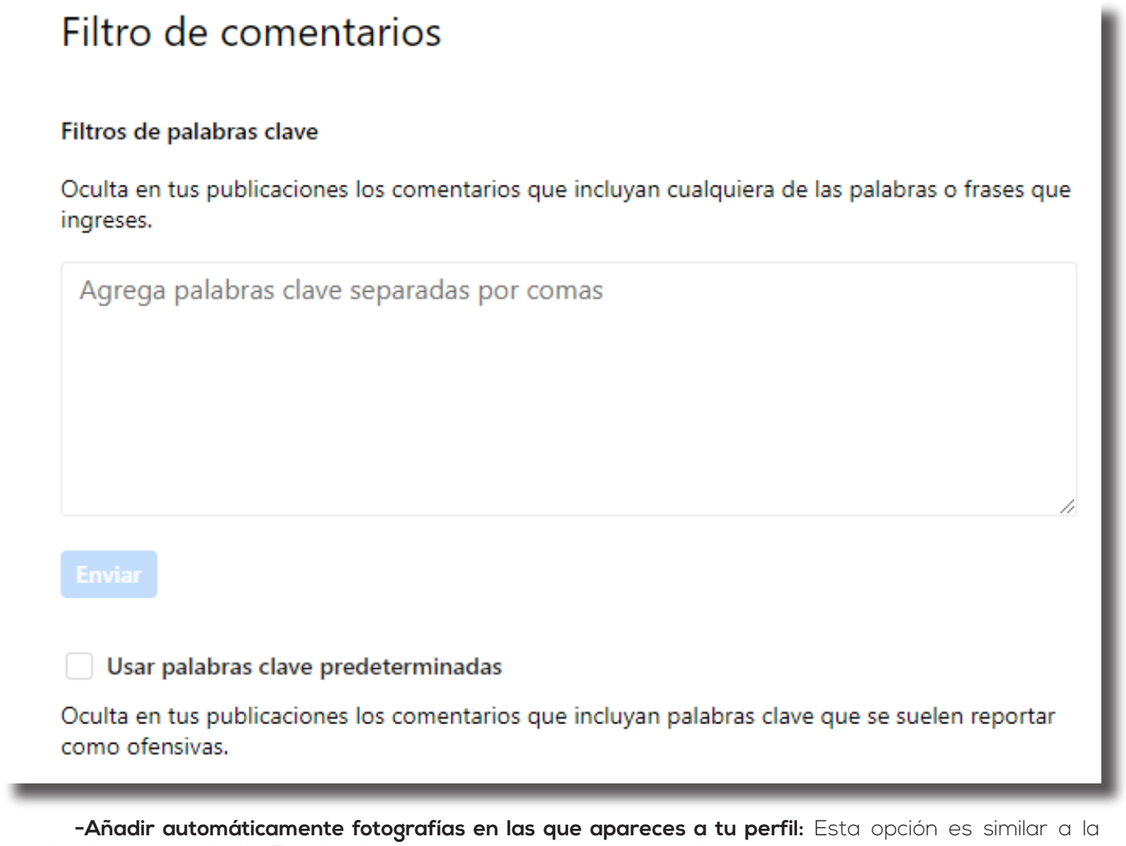
-Cuenta privada: En Instagram sólo existe el blanco o el negro, no hay variedades de gris como en las opciones de privacidad de Facebook. Esto implica que, o hacemos que nuestra cuenta sea totalmente pública, o totalmente privada.

Esto va a depender mucho del contenido que publiquemos en Instagram. Si vamos a hacer un uso de la red pensando sólo en nuestro círculo más cercano de amigos, conocidos y familiares, lo mejor es mantener la cuenta privada. De esta manera, cuando alguien quiera acceder a nuestro contenido, primero deberá enviarnos una solicitud para seguirnos. Si no aceptamos la solicitud, no podrá acceder al contenido que publiquemos.

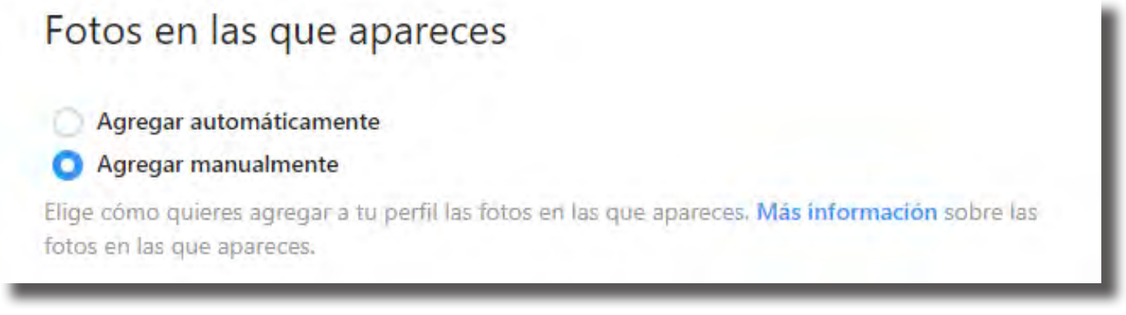
Si por el contrario, queremos enseñar al mundo el talento que tenemos, por ejemplo, con la pintura, entonces estableceremos la cuenta como pública, para que todo el mundo pueda contemplar nuestras obras de arte. Sin embargo, debemos ser muy cautos con el contenido que publicamos en esa cuenta, ya que, como hemos repetido, el contenido podrá ser visto por todo el mundo.

-Compartir historias: Podemos evitar que las historias que publiquemos, sean compartidas por otras personas, impidiendo de esta manera que el contenido se difunda sin control por Instagram.

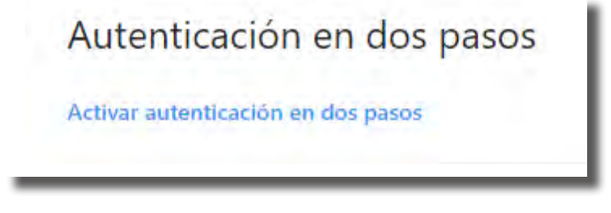
-Filtro de comentarios: Es útil si queremos evitar que ciertas palabras aparezcan en los comentarios de nuestras publicaciones. Podemos crear nosotros una lista o utilizar la que nos ofrece Instagram por defecto.



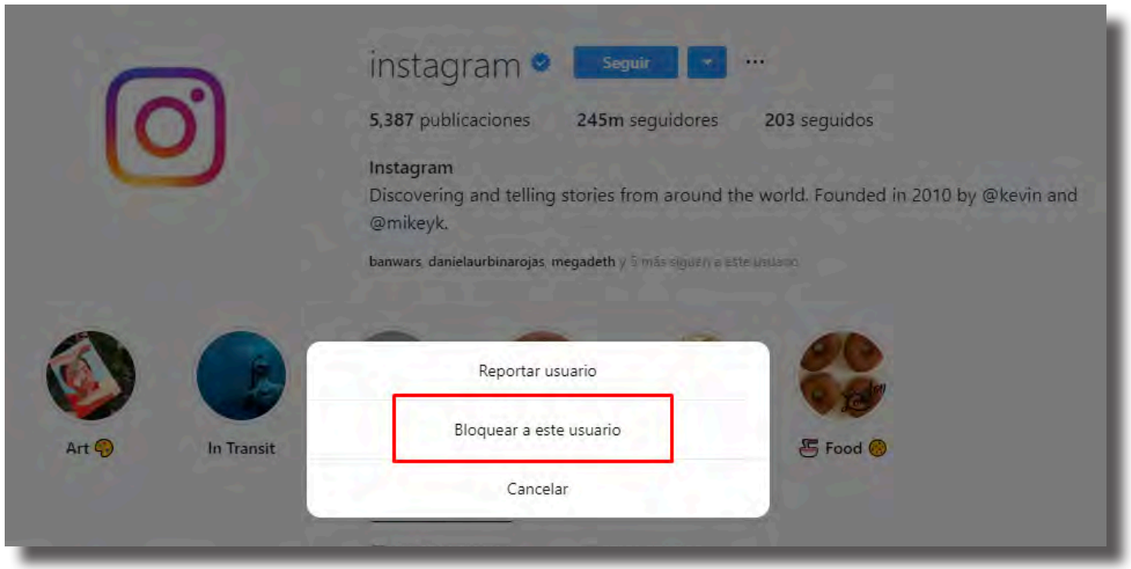
-Añadir automáticamente fotografías en las que apareces a tu perfil: Esta opción es similar a la revisión de etiquetado de Facebook sólo que, en este caso, no podemos evitar que nos etiqueten en una fotografía. El comportamiento por defecto de Instagram, es que en el momento en el que somos etiquetados, esa fotografía aparece en nuestro perfil. Si activamos la opción "Añadir manualmente", cuando se nos etiquete en una fotografía, podremos decidir si queremos añadirla o no a nuestro perfil. Es muy importante señalar, que Instagram permite eliminar etiquetas de una fotografía, por lo tanto, si aparecemos en una imagen o publicación en la que no queremos aparecer etiquetados, podemos eliminar esa etiqueta.



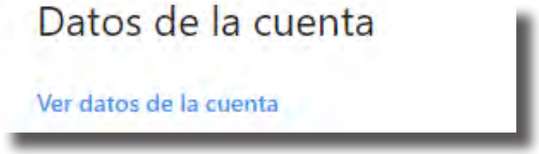
-Autenticación en dos pasos: Activar esta opción nos permitirá tener una mayor protección en nuestra cuenta, con el objetivo de que no sea robada.

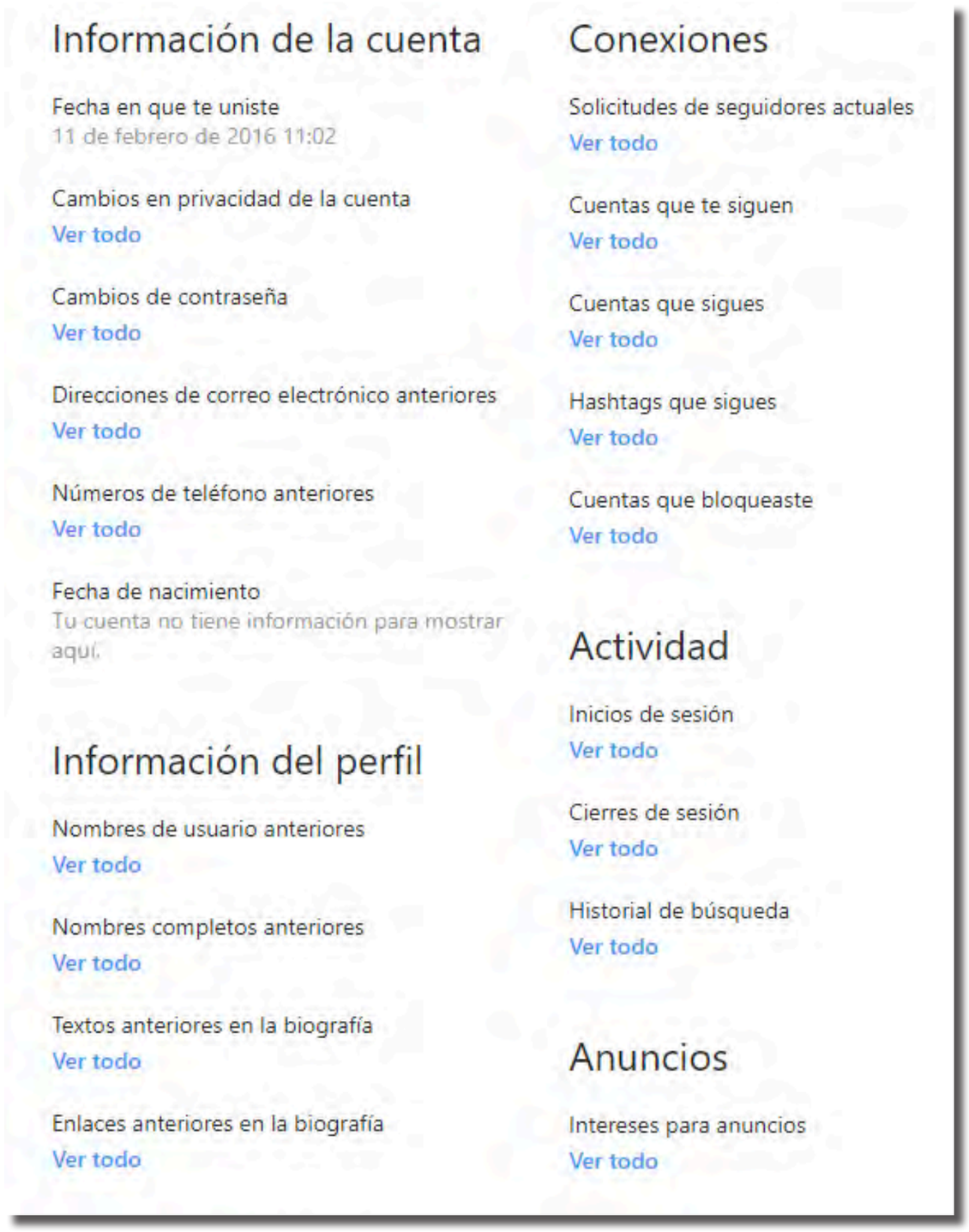


-Bloqueo de usuarios: Para bloquear usuarios, nos dirigiremos al perfil de la cuenta que queremos bloquear, y desde él podremos bloquearla. El proceso de desbloqueo es idéntico. Esto se puede hacer tanto a través de la web de Instagram, como en su aplicación para smartphones. Al bloquear a un usuario de Instagram, no podrá ver ninguna de nuestras publicaciones, así como tampoco podremos ver las suyas.



-Datos de la cuenta: En la versión para ordenadores, podremos acceder a mucha información relacionada con nuestra cuenta en este apartado:





Publicaciones cruzadas:

Una de las acciones que más realizamos cuando utilizamos las redes sociales, son las publicaciones cruzadas. Esto consiste en subir a más de una red social la misma publicación, generalmente compartiéndola.

Esto puede generar "agujeros" en la privacidad, y es algo que hay que tener en cuanta si queremos mantenerla.

Vamos a ver un ejemplo: Tu cuenta de Instagram la tienes en modo privado, de tal manera que sólo tus seguidores confirmados pueden ver tus publicaciones. Sin embargo, una de tus publicaciones en las que apareces con más gente, alguien la comparte en Twitter... En función de la configuración de Twitter de esa persona, la publicación que en principio era sólo para tus seguidores, se ha convertido en pública y accesible por cualquiera, pero no a través de Instagram, sino a través de otra red social, en este caso a través de Twitter.

La competición por los seguidores

Es habitual que nos encontremos con perfiles en Instagram con cientos o miles de seguidores. Constantemente vemos sus publicaciones y nos encantaría poder llegar a ese punto en el que está, teniendo muchas interacciones y comentarios en todas sus publicaciones.

Esto nos puede llevar a prácticas que no son muy recomendables, desde el punto de vista de la seguridad y la privacidad, debido al afán por conseguir más seguidores. En este caso debemos intentar:

-Seguir a cuentas indiscriminadamente esperando recibir el *follow-back, esto es el si te sigo me sigues.* En realidad no sabemos a quién estamos introduciendo en nuestra red cuando realizamos seguimientos indiscriminados.

-Utilización de servicios de compra de seguidores: Estos servicios ofrecen por un bajo precio, poder obtener de manera inmediata seguidores en nuestras redes sociales. En realidad esta práctica se trata de una estafa, y pueden llegar a cerrar nuestras cuentas por hacer uso de estos servicios. Hay que tener en cuenta que los seguidores que nos llegan de esta manera, generalmente son cuentas falsas que son eliminadas tarde o temprano, por lo que al final perderemos lo que nos hemos gastado en conseguirlos. Además conviene plantearse la conveniencia de contar con una legión de seguidores que en realidad son cuentas vacías. Realmente, los seguidores en una red social no miden el éxito que tenemos en nuestra vida, por lo tanto no te obsesiones con eso.

WhatsApp y Telegram, las redes sociales "tapadas"

Cuando hablamos de estas aplicaciones, generalmente las entendemos como aplicaciones de mensajería instantánea. Y con ese objetivo nacieron. Pero poco a poco, y tras las funcionalidades que han ido añadiendo, se han convertido en algo más que una aplicación exclusivamente para comunicarnos con otras personas.

De hecho ambas aplicaciones ya tienen la consideración de redes sociales, al permitir la interacción a través de grupos y permitir compartir imágenes, vídeos, documentos, enlaces, etc... Incluso WhatsApp tiene una funcionalidad similar a las stories de Instagram a través de los "estados".

Todas las recomendaciones que hemos ido dando son perfectamente aplicables a estas redes sociales, sin embargo, debido a su naturaleza tienen una serie de peculiaridades que debemos analizar. Estas redes sociales tienen una particularidad y es que cuando hacemos un uso responsable de ellas, ofrecen una medida adicional de seguridad. Esto es debido al hecho de que para tener una cuenta, es necesario tener un número de teléfono. Esto consigue que el número de cuentas falsas sea muy bajo y que las medidas de bloqueo sean muy efectivas.

La última frontera

Las aplicaciones de mensajería instantánea son la última frontera que separa el mundo virtual del mundo real. En el caso de WhatsApp para poder comunicarnos con otro usuario necesitamos conocer su número de teléfono. Esto puede implicar consecuencias negativas si no extremamos las precauciones a la hora de utilizar esta aplicación.

Generalmente, cuando entablamos relación con alguien lo primero que hacemos es agregarlo a nuestras redes sociales, lo seguimos en Instagram o Twitter lo agregamos como nuestro amigo en Facebook, etc... Sin embargo, si la relación se hace más estrecha llegamos al punto de intercambiarnos nuestros teléfonos para seguir conversando de manera más directa a través de WhatsApp.

Como hemos visto en las prácticas de riesgo, si un usuario malintencionado consigue llegar hasta esta "zona privada", tendrá acceso a muchísima más información sobre nosotros, pudiendo realizar su ataque de manera más sencilla.

Es por este motivo que debemos extremar las precauciones a la hora de utilizar esta aplicación con personas que hemos conocido a través de Internet, siguiendo unas pequeñas pautas, para evitarnos sorpresas desagradables.

-WhatsApp

A día de hoy WhatsApp es la aplicación de mensajería más extendida y utilizada del mundo, actualmente es propiedad de Facebook, quién de nuevo, ha intentado aplicar las mejoras de privacidad que ha venido aplicando en los últimos tiempos.

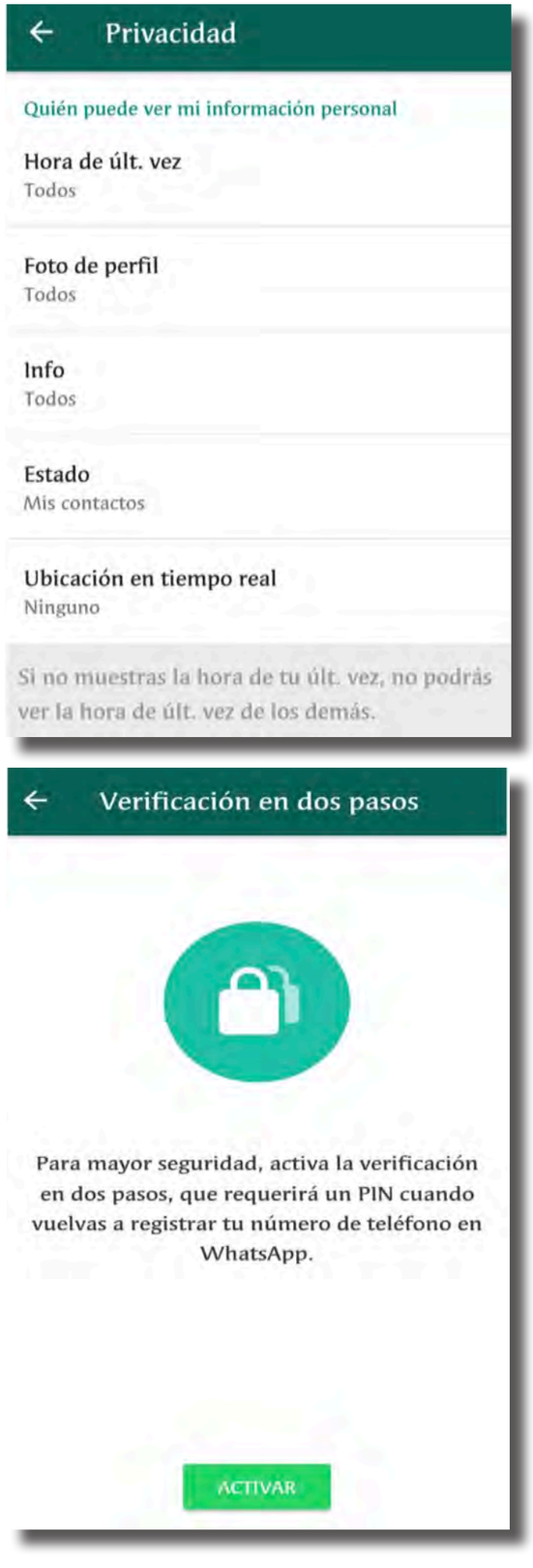
Actualmente esta aplicación permite la interacción con los usuarios de maneras muy diversas, y también nos ofrece múltiples opciones a la hora de configurar qué información queremos que se comparta con los demás.

Es muy importante saber configurar de manera correcta todas las opciones de privacidad que ofrece WhatsApp, con el objetivo de que personas que en realidad no conocemos no puedan acceder a esta información.

También tenemos que ser cuidadosos a la hora de interactuar con los grupos. En WhatsApp, no podemos interactuar con nadie si no es a través con su número de teléfono, por lo que tenemos que ser respetuosos con los demás, y preguntarles si quieren que los agreguemos a un grupo antes de hacerlo, ya que en él puede haber personas que no conozca, o no quiere que su número de teléfono se difunda a través de la red.

Las opciones de privacidad que recomendamos configurar son las siguientes:

- **Hora de última conexión:** Cuando un contacto accede a nuestro perfil o a las conversaciones



privadas, aparece la última hora en la que hemos estado utilizado la aplicación, ya sea conversando o leyendo mensajes. Este ajuste, útil en algunas circunstancias, también puede ser utilizado para obtener hábitos de uso o de horarios. Por eso, se recomienda establecerlo como mínimo en "Mis contactos". De esta manera, sólo números de teléfono que hayamos agregado a la agenda de nuestro teléfono, serán capaces de ver este dato.

- **Foto de perfil, info y estado:** Al igual que lo anterior, es recomendable establecer este ajuste como mínimo a "Mis contactos", con el objetivo de limitar la información disponible para personas a las que no conocemos.
- **Confirmaciones de lectura:** Realmente este ajuste depende de nosotros mismos, ya que si desactivamos las confirmaciones de lectura, para que las demás personas no puedan saber si hemos leído o no sus mensajes, también perderemos esa funcionalidad, y no podremos saber si los demás han leído nuestros mensajes.
- **Establecer verificación en dos pasos:** Los mensajes de WhatsApp no pueden ser accedidos por ninguna cuenta que no tenga el mismo número de teléfono. Es decir, no podremos configurar nuestra cuenta en otro móvil, si éste no tiene el número de teléfono asociado a nuestra cuenta. De esta manera, si alguien quiere leer nuestros mensajes, debe obtener acceso a nuestro teléfono. Pero en el caso de que una persona, consiguiera acceso a nuestro teléfono y lo pudiera reestablecer al estado de fábrica para poder hacer uso de él, podría instalar WhatsApp y leer nuestros mensajes. Para evitar éste inconveniente, podemos usar la verificación en dos pasos. Una vez establecida la clave, cuando se realice una instalación de WhatsApp, nos solicitará esta clave para completarla y acceder a nuestra cuenta. De esta manera, aunque perdiéramos nuestro teléfono, nadie podría acceder a nuestras conversaciones privadas, aún en el supuesto de que pudiese acceder a nuestro teléfono móvil.

SEGURIDAD EN EL TELÉFONO MÓVIL

Hemos hablado mucho sobre la seguridad de las cuentas de redes sociales, de correo electrónico o de otros servicios de Internet. Pero desde luego, uno de los elementos más importantes que tenemos que proteger, es nuestro Smartphone ya que hacemos un uso casi constante de él y aunque no nos demos cuenta, es un foco centralizador de todas nuestras cuentas.

Estos dispositivos almacenan gran cantidad de información sobre nosotros. Tenemos nuestras fotografías, el acceso a todas nuestras redes sociales que se efectúa de manera automática, el historial de navegación, nuestras conversaciones de WhatsApp, nuestra agenda, etc...

Prácticamente toda nuestra vida la llevamos hoy en día en nuestros teléfonos.

Por eso es muy importante que seamos capaces de proteger el acceso a esa información, ya que en cualquier momento podríamos perder el teléfono, o ser víctimas de un hurto.

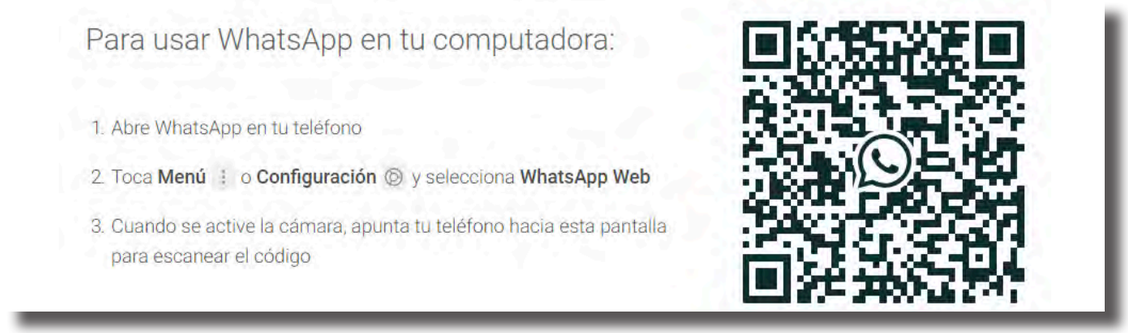
Para proteger el acceso a la información, lo principal es establecer un código de desbloqueo. Este código puede ir desde un número de 4 dígitos, hasta el reconocimiento facial de los modelos más actuales.

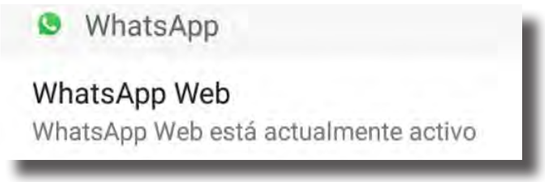
Debemos establecer, siempre que sea posible, el mecanismo de desbloqueo más restrictivo que podamos. Esta lista ordena, de menor a mayor nivel de protección, los diferentes métodos de desbloqueo que existen:

-Geolocalización
-Dispositivo Bluetooth
-Pin dígitos
-Contraseña
-Desbloqueo por reconocimiento facial
-Desbloqueo por huella dactilar

Hay que tener en cuenta, que tanto el desbloqueo por geolocalización, como el desbloqueo a través de algún dispositivo Bluetooth, entrañan ciertos riesgos, ya que no son precisos al 100% y existe la posibilidad de que por proximidad se pueda desbloquear el teléfono.

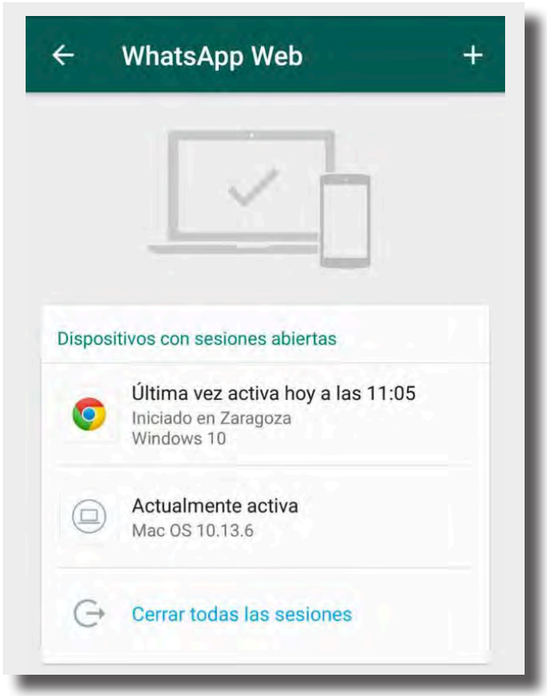
-WhatsApp Web y aplicación de escritorio: Una de las funcionalidades más útiles que tiene WhatsApp, es el hecho de poder utilizar la aplicación desde un ordenador, tanto a través de su página web, como de una aplicación para escritorio. Aunque no posee todas las opciones de configuración, debiendo realizar todas desde la app para móviles, sí que permite trabajar de manera más cómoda, sobre todo a la hora de compartir archivos con nuestros contactos.





El proceso para poder utilizar la aplicación en el ordenador, consiste en acceder a la web de WhatsApp o abrir la aplicación, y escanear el código QR que aparece con nuestro teléfono.

De manera inmediata, aparecerán nuestras conversaciones y nuestros contactos, y podremos chatear con ellos. A su vez, en nuestro teléfono, aparecerá una notificación que no podremos eliminar, informándonos de que WhatsApp web está abierto.



Además, todo lo que realicemos con la aplicación de escritorio, se sincronizará de manera automática con nuestro teléfono, por lo que no perderemos ninguna información, archivo o conversación.

Sin embargo, el riesgo de utilizar este método es alto, debiendo ser muy precavidos a la hora de utilizarla.

-Si dejamos la aplicación abierta en un ordenador, cualquiera que utilice el ordenador, podrá acceder a todas nuestras conversaciones, y a casi la totalidad de los archivos enviados a través de WhatsApp. Por eso es muy importante cerrar la sesión siempre que no estemos utilizando la aplicación.

Si por algún motivo no la hemos cerrado, cuando hemos dejado de utilizarla en el ordenador, podremos cerrar todas las sesiones desde el teléfono móvil, impidiendo de esta manera el acceso a otras personas.

-Telegram, la red social de los "bots"

Telegram es un servicio de mensajería instantánea, similar al popular WhatsApp que nació con la privacidad por bandera, y tal fue su aceptación que muchas de las opciones que traía en su primera versión, fueron incorporadas por WhatsApp posteriormente. Funcionalidades como el envío cifrado de las conversaciones, para que no pudieran ser interceptadas cuando enviamos un mensaje, o el cifrado de los archivos locales situaron a Telegram como la aplicación más respetuosa con la privacidad del usuario.

Actualmente, Telegram es muy usado por la funcionalidad que ofrecen sus grupos, los cuales permiten la participación de usuarios sin desvelar sus números de teléfono a los demás participantes. Gracias a esto, se están utilizando los grupos y canales de Telegram para diversas actividades, tanto lícitas, como ilegales.

Entre las actividades que se llevan a cabo en estos grupos, cabe destacar, el intercambio de archivos con derechos de autor, como música, películas, libros, series, etc...

Estos canales, habitualmente son gestionados por bots, programas informáticos que responden a las interacciones del usuario. Sin embargo, estos bots tienen en muchas ocasiones otros usos, como el engaño o la estafa.

Por eso, debemos mantener las mismas precauciones a la hora de pulsar en enlaces dentro de Telegram que cuando lo hacemos navegando a través de Internet, ya que cuando uno de estos enlaces es compartido en grupos o canales, en realidad no sabemos quién está enviando el enlace, ni con qué propósito.

VIDEOJUEGOS – LA AMENAZA LATENTE

Los videojuegos han llegado para quedarse, y todos, en mayor o menor medida, hemos utilizado alguna vez un videojuego, ya sea usando una videoconsola, un ordenador o un teléfono móvil.

En la actualidad, los videojuegos son más sociales que nunca, y permiten una interacción con los demás jugadores que no se había producido anteriormente. Esto, además de ser una buena manera de interactuar entre personas, creando nuevas amistades y relaciones, ha generado en nuestras casas y nuestros bolsillos un nuevo vector de ataque, que los delincuentes pueden utilizar para amenazar nuestra seguridad.

Hay que tener en cuenta, que los videojuegos van dirigidos principalmente a uno de los sectores de la juventud más vulnerables, y necesitan ser tratados con responsabilidad y sentido común. No dejan de ser una herramienta más dentro de nuestro tiempo de ocio, no debiendo convertirse en la única opción de divertimiento.

Además, alrededor de los videojuegos se ha creado todo un nuevo movimiento social, creando todo un nuevo ecosistema relacional. Gracias a los videojuegos, plataformas como Twitch, en la cual se pueden retransmitir nuestras partidas para que otros usuarios la vean e interactúen con nosotros en directo, han alcanzado un gran éxito. Además, en YouTube, la red social de almacenamiento de vídeos, los canales que más visitas reciben y más suscriptores tienen son los relacionados con los videojuegos.

Tiene también especial relevancia todo el mundo de los e-sports o deportes electrónicos, los cuales están moviendo gran cantidad de jóvenes, atraídos por las grandes estrellas de sus juegos favoritos. Ya existen campeonatos mundiales de videojuegos como League Of Legends, DOTA 2, Counter Strike, etc... Y cada vez es mayor el público que acude a verlos y que participa de manera activa durante toda la temporada competitiva.

Todo esto crea un marco perfecto para todas aquellas personas que quieren aprovecharse de la vulnerabilidad y exposición de los más jóvenes ante esta nueva realidad, por lo que debemos extremar las precauciones y estar siempre vigilantes en busca de comportamientos que puedan generar sospechas.

A lo largo de esta carpeta, hemos enumerado la cantidad diferente de formas que existen de acoso, extorsión y engaño. Todas ellas son aplicables en el mundo de los videojuegos. Existen plataformas como Steam, que por la cantidad de usuarios que tiene y por el grado de interacción que existe entre ellos, podrían considerarse ya redes sociales.

También hemos contado lo sucedido con el juego Pokemon Go, puesto anteriormente de ejemplo de mal uso de la tecnología, o los engaños realizados con Fortnite, usado como reclamo para conseguir estafar a los usuarios desprevenidos. Pero por supuesto, existen multitud de casos similares, que lo único que buscan es engañar y estafar a los usuarios.

Estos engaños pueden ir desde los más sofisticados, por ejemplo, usando un nombre confuso que copie el de algún videojuego famoso para intentar engañar a los usuarios y que descarguen el videojuego equivocado, hasta los anuncios que prometen que conseguiremos más objetos en el juego o que seremos mejores si compramos sus productos, conocidos también como *cheats* (trucos). Estos programas que permiten mejorar en un videojuego, son totalmente ilegales, y su uso puede suponer que eliminen nuestra cuenta del juego de por vida.

También existen páginas web, que sabedoras del hecho de que el poder adquisitivo de los usuarios habituales de videojuegos es bajo, obtienen claves de manera ilegal y las revenden mucho más baratas que compradas en los sitios oficiales. Si compramos en estas páginas de keys, corremos el riesgo de que el juego sea eliminado de nuestra cuenta, enfrentándonos en los casos más graves, a la pérdida de toda ella, impidiendo el acceso a todos los demás productos que tuviéramos comprados.

Por todo esto es importante tener en cuenta que, cuando veamos ofertas que parecen increíbles, prometen cosas que sabemos que son prácticamente imposibles o sospechamos que un videojuego quizás no sea el que dice ser, debemos consultar fuentes fiables, preguntar a un adulto o consultarlo con la comunidad de jugadores, que normalmente proporcionan ayuda y consejos útiles.

Sin embargo, la mayor amenaza que tienen los videojuegos son los problemas derivados de su abuso. En junio de 2018 la Organización Mundial de la Salud, incluyó en el listado de enfermedades la adicción a los videojuegos como un desorden de salud mental.

Y la realidad es que la adicción a este tipo de productos puede ser muy perjudicial, ya que los problemas se presentan tanto a corto como a largo plazo.

El titular que hizo saltar todas las alarmas, una niña de 9 años en rehabilitación por su adicción a los videojuegos.

En Junio de este año, saltó la noticia, una niña de 9 años se encuentra en rehabilitación debido a la adicción a un videojuego. Este comportamiento insano, había llevado a la niña a estar más de 10 horas seguidas jugando, llegando a orinar encima por no abandonar la partida para ir al baño.

Desde hace un tiempo, los padres habían notado que la niña no se comportaba como de costumbre, se dormía en clase, se enfrentaba a sus padres cuando amenazaban con quitarle la videoconsola y descendió muchísimo su rendimiento escolar. Además, esta niña, que hasta entonces había sido muy aficionada a practicar deporte, había abandonado por completo esta actividad.

Los padres tardaron tiempo en darse cuenta, porque la niña esperaba a que éstos se durmieran para levantarse a jugar por la noche. De ahí que por el día la niña estuviera cansada constantemente.

Como podemos ver, son comportamientos totalmente identificables y compatibles con el comportamiento bajo los efectos de una adicción severa.

El uso abusivo de los videojuegos, como de cualquier otra actividad, puede ser muy dañino para la salud, algunos de los riesgos asociados a su uso son:

- -Sedentarismo
- -Pérdida de relaciones sociales
- -Exposición a contenidos inapropiados
- -Posición de vulnerabilidad frente a otros usuarios

Además, los modelos de negocio de los videojuegos más populares incitan al juego. En la actualidad los videojuegos más populares no cuestan dinero para poder jugar a ellos, sin embargo, ofrecen multitud de objetos dentro del mismo, o bonus de algún tipo para conseguir ventajas, o acceso a nuevas funcionalidades de manera anticipada previo pago.

Sobre todo, en juegos para teléfonos móviles, muchas veces los editores crean limitaciones en el tiempo al número de partidas que se pueden jugar, o al número de objetos que se pueden conseguir, necesitando pagar dinero para acelerar estos procesos.

Esta práctica que va dirigida a los más jóvenes, puede generar situaciones de gasto descontrolado, ya que, por norma general, este tipo de juegos no imponen límites a la hora de las compras, pudiendo acumular objetos de manera indefinida. Además, constantemente incitan a estas compras a través de ofertas, promociones o dando la sensación que cuando no se paga se detiene el avance o la competitividad.

De estos casos tenemos ejemplos muy recientes, como el de un joven canadiense que gastó aproximadamente 7000€ en un mes en el famosos videojuego FIFA 17, o el caso de un japonés, que gastó aproximadamente 6000€ en una noche, intentando conseguir un personaje para un juego de éxito en su país.

Estos casos demuestran que cuando se hace un uso descontrolado e irresponsable de los videojuegos, se pueden generar situaciones muy peligrosas y perjudiciales para los más jóvenes. Por eso es muy necesario ser conscientes de estas prácticas de riesgo, y estar atentos a cualquier signo que pudiera derivar en una adicción mucho más severa.

4 guía de **buenas prácticas**

BUENAS PRÁCTICAS A LA HORA DE COMPRAR POR INTERNET

Durante toda esta guía hemos estado poniendo el foco en los riesgos derivados del malware, de cómo debemos proteger nuestras cuentas on-line, de las prácticas de riesgo en redes sociales y la amenaza latente de los videojuegos. Podríamos decir que estos riesgos son los derivados del uso de Internet, amenazas existentes por el mero hecho de utilizar los servicios en red y los dispositivos que usamos para acceder a él.

Otra de las prácticas más habituales, la cual muchos de los usuarios de Internet hemos realizado alguna vez, es la compra on-line.

Esta nueva manera de adquirir productos o servicios, ha generado toda una nueva serie de amenazas y riesgos que debemos tener en cuenta a la hora de realizar compras de manera segura, para evitar caer en estafas, engaños o robos.

Actualmente las compras a través de Internet están en alza frente al comercio tradicional, esto es debido a las múltiples ventajas que ofrece la compra on-line:

- Mayores posibilidades de comparar precios.
- Facilidades en la entrega y devolución de los pedidos.
- Precios más competitivos u ofertas más significativas.
- Gran información disponible sobre el producto que vamos a comprar.

Aunque las medidas de protección contra el fraude y el conocimiento que tiene el consumidor son mayores, todavía se siguen produciendo miles de casos de estafa. A continuación te daremos una serie de recomendaciones y consejos para no ser engañado, y te facilitaremos un listado con los métodos de pago más seguros, para que realices tus compras a través de Internet con total confianza y seguridad.

La confianza es la clave

Procura realizar tus compras en páginas web que inspiren tu confianza. Webs a medio hacer, con muchas faltas de ortografía, sin identificativos claros de la empresa o su ubicación, son generalmente síntoma de que la compra no va a salir como nosotros queremos. Es importante señalar, que debido a la ley de servicios de la sociedad de la información, todo comercio online está obligado a informar sobre los datos de la empresa. Esto incluye su nombre o denominación social, su número de identificación fiscal, su dirección, datos relativos a la inscripción en el registro mercantil, correo electrónico, y un medio de contacto para establecer comunicación directa y efectiva (un formulario de contacto o un teléfono, por ejemplo). Si estos datos no aparecen, o están confusos y poco visibles, hay que prestar mucha atención, ya que podríamos estar ante un engaño.

Además, las tiendas on-line deben dar información sobre todo el proceso de compra, las condiciones en las que se va a efectuar y además deben proporcionar información de forma detallada sobre la manera en que se van a tratar tus datos personales.

Otro dato de especial relevancia a la hora de confiar más o menos en una tienda on-line, es la presencia tanto del sello de confianza on-line, otorgado a las empresas que se han adherido a un código ético de conducta, y han pasado un test realizado por una organización independiente. También es importante el hecho de que la página web tenga un certificado HTTPS, el candado verde que aparece en el navegador cuando accedemos a una página web que lo tiene instalado. De esta manera sabremos que estamos accediendo a una página web real, cuya veracidad ha sido certificada por organismos competentes, siendo muy improbable que la página web no sea falsa.

Como medida adicional, podemos buscar información de la tienda on-line en concreto. Si están disponibles, conviene proceder a la lectura de opiniones de otros usuarios acerca de la tienda y los productos que ofrece, para conocer lo que opinan de ella, y saber si es o no fiable.

A su vez, estas opiniones no deben ser nunca la única base para fiarnos o no sobre una página web, ya que las opiniones pueden estar sesgadas o incluso ser falsas, con el propósito de dar credibilidad a una web falsa, o incluso de hacer descender la reputación de una web por parte de un cliente descontento. Es por lo tanto muy necesario que al realizar esta comprobación consultes varias fuentes, y que éstas tengan buena reputación.

Ofertas trampa

Hay que tener cuidado cuando aparezcan ofertas que parezcan demasiado buenas para ser ciertas, en muchas ocasiones sólo serán reclamos para atraer visitantes a una página web, y en otras directamente serán estafas, dónde una vez pagado el producto, jamás recibiremos lo que hemos comprado, o recibir algo que en nada o muy poco, se parece a lo que realmente se estaba ofreciendo, como productos de imitación o falsificaciones.

De nuevo, la información es la clave. Consultar precios de productos similares en páginas web de confianza o encontrar buenas opiniones sobre la tienda que ha publicado la oferta, son indicadores de que la oferta puede ser real. Sin embargo, si no encontramos otro precio similar, o sí la página web sólo tiene valoraciones negativas, o ni siquiera existen opiniones en Internet sobre ella, es posible que se trate de un engaño.

CÓMO PAGAR POR INTERNET

Para poder efectuar nuestras compras por Internet de la manera más segura posible, existen herramientas que nos permitirán hacerlo, y lo que también es importante tener en cuenta, sin suponer un coste adicional para nosotros.

Lo más recomendable siempre es utilizar medios de pago que tengan limitado el dinero que se puede utilizar, de tal manera que en caso de que sufriéramos un robo de nuestros datos, el robo sería únicamente por la cantidad que tuviéramos limitada.

También es importante tener en cuenta de qué manera se realiza el pago en la página web o aplicación en la que estamos comprando. Cuando para completar un pago, lo tenemos que hacer a través de la página web de nuestro banco, da garantías de que nuestros datos de pago no van a caer en malas manos, ya que el pago lo realiza el banco, y no va a ceder nuestros datos a terceros.

En los pagos con tarjetas bancarias a través de Internet, también existe la posibilidad de que el banco te ofrezca la autenticación de doble factor a la hora de realizar un pago, de esta manera, para completar la operación, además de la información de nuestra tarjeta, el banco nos enviará un código a nuestro teléfono para completar la operación. Al realizar el pago en una tienda on-line, se nos redirige a lo que se conoce como pasarela de pago, que no es más que una página web de nuestro banco en la que debemos introducir un código que nos enviaran al teléfono móvil asociado con la tarjeta que estamos usando para confirmar o efectuar el pago.

Tarjetas monedero

Una tarjeta monedero es simplemente una tarjeta de débito especialmente pensada para pagar por Internet. Estas tarjetas funcionan como un monedero dónde se almacena el dinero que nosotros recargamos. En caso de que los datos de nuestra tarjeta cayeran en manos de delincuentes y la usaran para realizar compras de manera fraudulenta, sólo podrán quitarnos el dinero que tuviera la tarjeta en ese momento.

De manera general todos los bancos ofrecen este servicio, siendo además sin coste adicional, por lo que es muy recomendable realizar los pagos de esta manera.

Servicios de pago on-line

En Internet, existen varias empresas que realizan la función de intermediarios a la hora de pagar, son como monederos totalmente virtuales, siendo el más famoso PayPal.

Estas plataformas de pago, requieren que abramos una cuenta con nuestros datos, pudiendo recargar el dinero que tenemos disponible para efectuar nuestras compras. Las ventajas que ofrecen son muchas, entre ellas:

- Cuando realizamos una compra utilizando estos servicios, nosotros no le pagamos al comprador, sino que la plataforma es la que realiza el pago, posteriormente nosotros le pagaremos a la plataforma.
- Ofrecen protección al comprador, de tal manera que si hemos realizado una compra y ésta no coincide con lo que hemos pagado, o ni siquiera llegamos a recibirlo, podemos reclamar al vendedor a través de la plataforma. De manera general siempre recuperaremos el dinero que hemos perdido.

Aunque también hay que tener cuidado a la hora de utilizar estos servicios, ya que, si no protegemos nuestra cuenta de manera correcta, usando contraseñas fuertes, habilitando la autenticación de doble factor, etc... Hay que tener en cuenta que, si alguien consigue acceso a nuestra cuenta, podría utilizarla para realizar compras en nuestro nombre para él mismo, y será muy difícil demostrar que no hemos sido nosotros quienes las hemos realizado.

Tarjetas prepago

Las tarjetas prepago son el método de pago más seguro actualmente. Esto es debido a que la compra de las tarjetas las podemos incluso realizar en tiendas físicas con dinero en metálico. El problema es que sólo unas pocas tiendas o servicios en Internet ofrecen esta posibilidad.

Sin embargo, plataformas como Play Store de Android, o App Store de Apple, sí que permiten recargar dinero en nuestras cuentas a través de este sistema.

Para realizar los pagos de esta manera, es muy sencillo, adquirimos nuestra tarjeta de recarga en un establecimiento, esta tarjeta puede variar en precio, por lo tanto varía la cantidad de dinero que tendremos disponible para gastar.

Una vez tengamos la tarjeta, entramos en nuestra cuenta del servicio correspondiente, introduciremos el código que aparece en la tarjeta de prepago e inmediatamente aparecerá el dinero en nuestra cuenta con el cual podremos comprar lo que queramos.

Como decimos, probablemente este método de pago sea probablemente a día de hoy el más seguro de todos, por lo tanto, siempre que sea posible, es interesante utilizarlo. Como siempre la seguridad en éste cao también dependerá de lo segura que sea nuestra contraseña en el servicio en el que realizamos la recarga.

Tiendas on-line que almacenan tus datos de pago

En determinadas ocasiones, cuando realices una compra por Internet en una tienda on-line, te ofrecerán la posibilidad de almacenar tus datos de pago para futuras compras. De esta manera, si volvemos a comprar algo en esa tienda, no tendremos que volver a introducir los datos y el proceso de compra será más rápido y cómodo para ti.

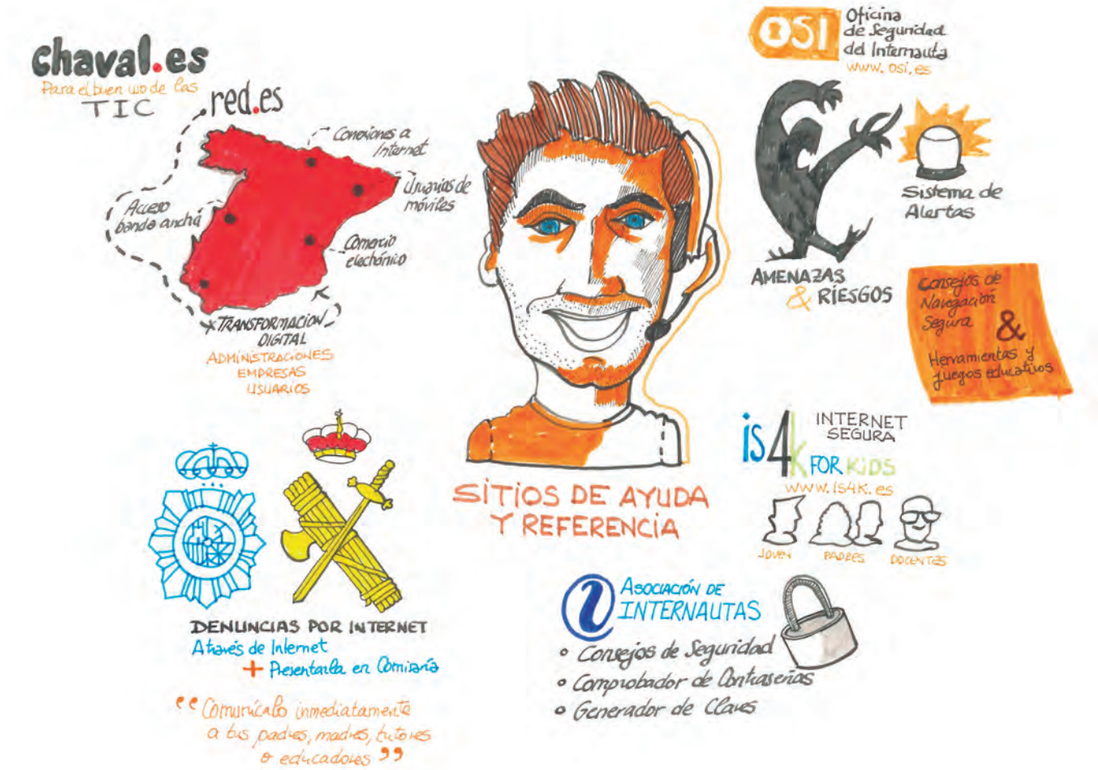
Sin embargo, el riesgo de hacer esto es alto, ya que al tratarse de información tan sensible como los datos de pago, cualquier problema o brecha de seguridad que tuviera esta página web, podría dejarnos expuestos a un robo bancario.

Por eso, es muy importante no almacenar los datos en ninguna tienda on-line, aunque sea más incómodo realizar las compras de esta manera, tenemos que priorizar la seguridad en estos casos.

Hay tiendas on-line, generalmente las más grandes, que almacenarán nuestros datos sin posibilidad de negarse, cuando esto suceda, lo recomendable es solicitar el borrado. De esta manera además de protegernos frente a posibles robos de información, también nos protegeremos frente a servicios de suscripción que en ocasiones nos intentan "colar" estas tiendas.

En caso de que queramos que nuestros datos se queden almacenados, debido al volumen de compras que realizamos en esta tienda, debemos intentar asegurarnos que la tienda tiene y cumple con los estándares de seguridad más exigentes, y realizar una búsqueda en Internet, para comprobar si la tienda ha sufrido en alguna ocasión algún tipo de robo de datos o algún incidente de seguridad.

SITIOS DE AYUDA Y REFERENCIA



Como hemos visto a lo largo de toda esta carpeta, los riesgos existentes en Internet y las redes sociales, se pueden presentar de muchas formas diferentes. Desde virus o malware hasta usuarios malintencionados que quieren robar nuestros datos o nuestro dinero, los métodos para ser víctimas de estos delitos son muchos y varían enormemente con el tiempo.

En este juego del gato y el ratón, entre las autoridades y los delincuentes, estos últimos invierten mucha cantidad de tiempo y de recursos para burlar las medidas de seguridad que aparecen diariamente y conseguir realizar sus acciones ilícitas.

También es prácticamente seguro, que dentro de un tiempo, muchas de las cosas que hemos comentado aquí ya estarán obsoletas, y habrán aparecido nuevos vectores de ataque que no se habían tenido en cuenta, o bien aparecerán nuevos tipos de ataque gracias a los avances tecnológicos que se producen de manera constante.

Por eso queremos señalar en este último apartado, los sitios de referencia y los procedimientos que existen en Internet para consultar las últimas amenazas que se han detectado, y que de tal forma, podamos denunciar a las autoridades. Así, entre todos, podemos poner freno a estos riesgos, y podremos disfrutar de todas las ventajas que ofrece Internet de forma segura.

OSI – Oficina de seguridad del internauta

Este organismo oficial, el cual forma parte de INCIBE (Instituto Nacional de Ciberseguridad), es el encargado de publicar de manera periódica las amenazas y riesgos más peligrosos a través de su sistema de alertas.

Además, en su página web www.osi.es podemos encontrar consejos de navegación segura, herramientas y juegos educativos que reforzarán nuestros conocimientos para poder realizar un uso más seguro de Internet.

Dentro de esta oficina, también se encuentra la iniciativa Internet Segura for Kids, www.is4k.es Esta herramienta se dirige a los usuarios más jóvenes y a sus padres así como a docentes, brindando información, concienciación y consejos sobre cómo hacer un uso responsable y seguro de Internet. Informando, además, de los riesgos y amenazas existentes para los más pequeños, dándonos consejos sobre cómo evitarlos, detectarlos y denunciarlos.

Asociación de Internautas

Esta asociación intenta proteger los derechos de los internautas en lo referente al acceso y uso libre de Internet como medio de información. En los últimos tiempos también se dedica a difundir consejos de seguridad y dispone de herramientas útiles como un comprobador de contraseñas, para medir su fuerza o un generador de claves, que nos puede servir para generar nuestra contraseña maestra.

RED.ES

Enmarcado dentro del Ministerio de Economía y Empresa, se encuentra la plataforma red.es (www.red.es). Esta iniciativa se dedica a la transformación digital del país y ayuda a administraciones, empresas y usuarios a adaptarse a las nuevas tecnologías.

Una parte fundamental dentro de esta transformación digital, es la seguridad y protección de los usuarios de Internet, para lo que han creado la plataforma www.chaval.es la cual se encarga de difundir el buen uso de las TIC tanto a padres, como a tutores o educadores, informando sobre las ventajas y posibles riesgos de las tecnologías que existen para los jóvenes.

Denuncias por Internet

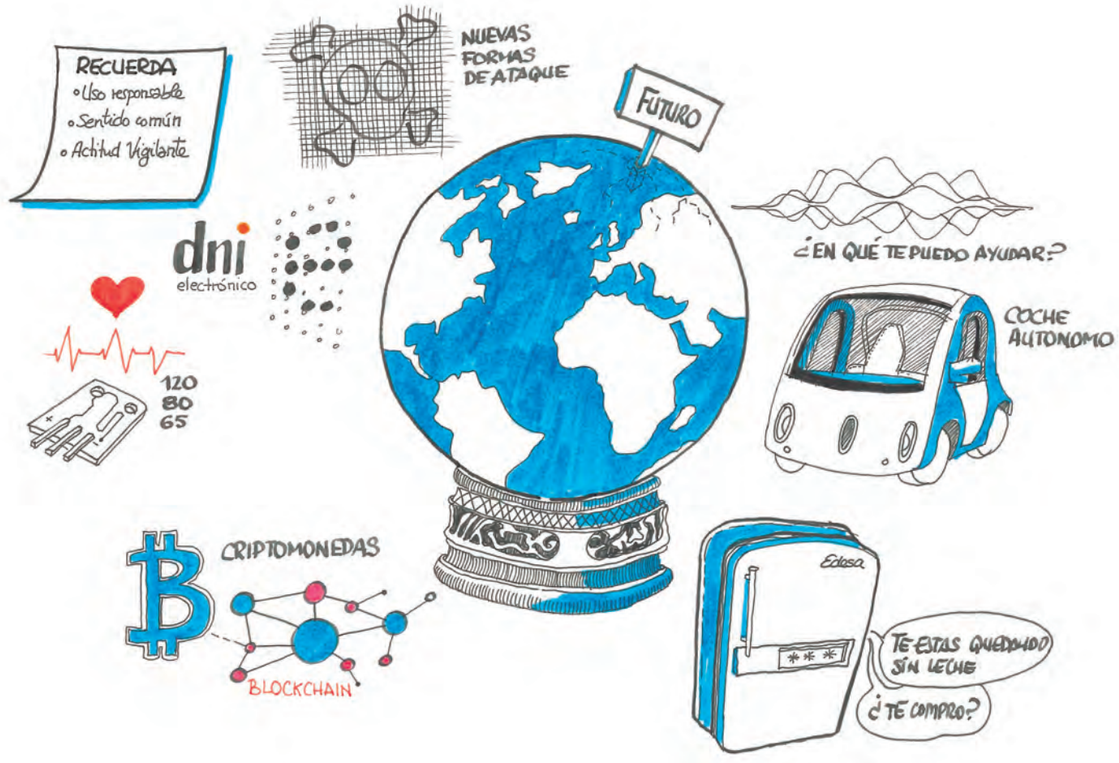
Es posible que, en algún momento nos encontremos con un hecho que pueda ser constitutivo de delito. Cuando estemos delante de este hecho, es muy importante que lo comuniquemos de manera inmediata a nuestros padres, madres, tutores o educadores. Hay que tener en cuenta que los delitos cometidos a través de Internet, son igualmente punibles y serios que los realizados en la vida real.

Llegado el caso de tener que denunciar un hecho del que hayamos tenido constancia a través de Internet, o que estemos sufriendo o que esté sufriendo alguna persona cercana a nosotros, la denuncia también podemos hacerla a través de Internet.

Tanto la policía nacional, como la guardia civil, permiten presentar una denuncia a través de Internet, de tal manera que podamos denunciar el hecho que hayamos visto de manera inmediata.

Hay que tener en cuenta que cuando realizamos este tipo de denuncias, no basta con realizarlas a través de Internet, posteriormente tendremos que presentarla en una comisaria, para que tenga total validez.

No sólo hay que pensar en delitos como el acoso o el robo, es posible que nos encontremos con una página web que comparte contenidos ilegales o que pudieran estar protegidos por derechos de autor. O incluso podemos encontrarnos una web que intenta realizar phishing contra una entidad bancaria, por ejemplo. Cualquier de estos hechos puede suponer un delito, y es nuestro deber, si queremos mantener una red más segura y útil, denunciar estas prácticas.



¿Y el futuro...?

Internet cada día va a estar más presente en nuestras vidas, vamos a poder realizar compras simplemente hablando a un altavoz, e incluso llegaremos a ver coches autónomos circulando por nuestras calles. Todos los aparatos de nuestras casas estarán conectados a Internet, y podremos realizar acciones hasta ahora inimaginables, por ejemplo, que nuestra nevera realice un pedido a una tienda on-line cuando detecte que nos quedamos sin leche o cualquier otro producto de manera automática.

Es posible que veamos desaparecer el dinero físico, dejando paso a las criptomonedas como método de pago. Incluso es posible que ya no tengamos que firmar nunca más un contrato en papel, gracias a la tecnología del blockchain y sus smart contracts.

Poco a poco se irán reduciendo los trámites con las administraciones públicas que debemos hacer de manera presencial, pudiendo realizarlos a través de Internet gracias al D.N.I. electrónico.

Es posible que veamos nuevos avances en medicina en poco tiempo, empezando a generalizarse los implantes que controlen nuestra salud, pudiendo consultarlos en tiempo real. Incluso se llegarán a realizar diagnósticos de manera automática, cuando estos sensores puedan comunicarse de manera directa con los servicios de salud.

Sin embargo, todos estos avances, traerán consigo nuevas formas de ataque en contra de nuestra privacidad y seguridad. Por supuesto que las soluciones de seguridad serán cada vez más completas y ofrecerán multitud de opciones para mantenernos a salvo de estos ataques, aun así, siempre tendremos que considerarlas como un complemento a nuestra seguridad, siendo al final nosotros mismos responsables de ella.

El uso responsable de la tecnología, el sentido común a la hora de realizar determinadas acciones, mantener una actitud siempre vigilante ante cualquier sospecha que pudiéramos tener y consultar fuentes oficiales y fiables sobre las últimas amenazas que existen en Internet, nos ayudará muchísimo a tener una experiencia de uso segura y saludable.

CONTENIDO

1. Nuevas amenazas en la sociedad de la información 5

Medidas de proteccion contra virus (malware). 7

Otras amenazas en internet 9

2. Telefonía móvil 11

Otro tipo de comunicaciones 14

Otros dispositivos conectados 14

Otras medidas de seguridad 15

Buenas prácticas y sugerencias a la hora de establecer contraseñas para nuestras cuentas 16

3. Servicios en la "nube" 18

¿Qué es la nube? 19

Redes sociales 24

Videojuegos - La amenaza latente 44

4. Guía de buenas prácticas 46

instituto aragonés de la juventud

HUESCA
San Jorge, 65
22003
974 247 320
iajhuesca@aragon.es

TERUEL
Yagüe de Salas, 16
44001
978 624 440
iajteruel@aragon.es

ZARAGOZA
Franco y López, 4
50005
976 716 810
iaj@aragon.es

informacion.iaj@aragon.es
http://juventud.aragon.es
IAJota
Juventudaragon
de 9 a 14 horas,
de lunes a viernes

juventud
instituto aragonés de la juventud

■ Edita: Departamento de Ciudadanía y Derechos Sociales. Instituto Aragonés de la Juventud ■ D.L.: Z-183/93 ■ ISSN: 1136-887X ■ Imprime: Sistemas de Impresión, Industrias Gráficas, S.L. ■

GOBIERNO DE ARAGON