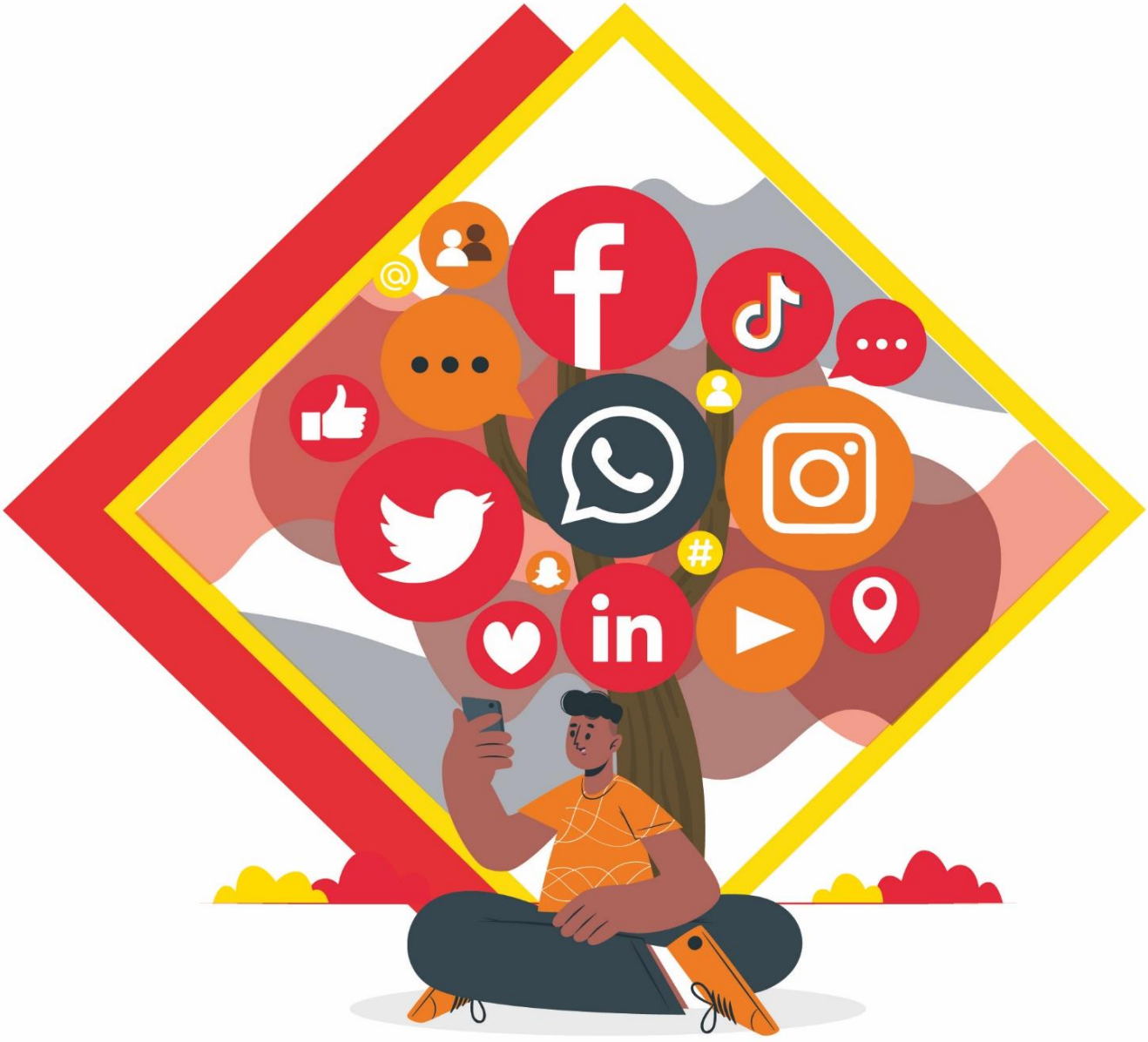
INSTITUTO NACIONAL DE CIBERSEGURIDAD

GESTIÓN DE LA PRIVACIDAD, IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE EN INTERNET

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

MÓDULO 2

Redes sociales y riesgos asociados



ÍNDICE

1. ¿Qué son las redes sociales y las aplicaciones de mensajería instantánea (MI)?

1.1 ¿Qué son las redes sociales y las aplicaciones de mensajería instantánea (MI)?

Una red social es un espacio virtual que facilita a los usuarios comunicarse entre ellos, establecer contactos, compartir y consumir contenidos y crear comunidades. Una de las características fundamentales de las redes sociales es la capacidad de democratizar la información, convirtiendo a los usuarios en receptores y productores de contenidos al mismo tiempo.

Los sistemas de mensajería instantánea no son solo considerados **plataformas de comunicación**, sino también **redes sociales**, ya que aparte de ser sistemas de mensajería de persona a persona, se pueden formar grupos de amigos o intereses, compartir toda clase de información, y ser usados en diferentes plataformas y dispositivos, como portátiles, móviles o tabletas. Además, también son consideradas plataformas de **comunicación masiva** al poder generarse comunidades de personas que comparten intereses o afinidades.

Las redes sociales, en general, permiten ser configuradas según nuestras preferencias a través de las opciones de seguridad y privacidad, como, por ejemplo, decidir si queremos crear un perfil público (al que todo el mundo tendrá acceso) o privado (sólo accesible a nuestros contactos). Cada usuario es responsable de la información que comparte, bien sea sobre sí mismo o sobre terceros.

Registrarse en una red social suele ser bastante sencillo, normalmente sólo es necesario rellenar un formulario con algunos datos personales y establecer un nombre de usuario y una contraseña para poder acceder. En la mayoría de redes sociales se establece una edad mínima para poder crear un perfil, variando según la red social. También hay que tener en cuenta que cada país tiene sus propias normas con respecto a la edad mínima para tener un perfil. En el caso de España, la Ley de Protección de Datos Personales y garantía de los derechos digitales establece que la edad mínima permitida para crear un perfil es de 14 años. ¿Qué ocurre si un menor de 14 años quiere crear un perfil en las redes sociales? En ese caso, sería obligatorio el permiso expreso de los padres o tutores legales.

Para administrar de manera más sencilla las redes sociales, existen una serie de aplicaciones conocidas con el nombre de **gestores de redes sociales**.

Un gestor de redes sociales es una herramienta, generalmente online, desde la que se puede administrar de una manera fácil y práctica las publicaciones en las redes sociales. Para utilizarlas tienes que darte de alta en la plataforma web e ir añadiendo diferentes perfiles de redes sociales. Hay que tener en cuenta que pueda haber limitaciones y diferencias en el caso de usar una cuenta gratis frente a una cuenta *premium* o de pago. En todo caso, podrás gestionar diferentes redes sociales, realizar publicaciones instantáneas o programarlas. También puedes realizar informes y análisis sobre el rendimiento de tus redes sociales (seguidores, *likes*, etc.).

Los expertos y profesionales de redes sociales usan habitualmente estas aplicaciones. Sobre todo, profesionales que se encargan de gestionar las estrategias de marketing digital de una marca.

A continuación, se muestra una tabla donde se especifica el nombre, año de creación, fundadores, características principales y la edad mínima de acceso de algunas de las redes sociales más usadas tanto a nivel personal como profesional.

Nota: con independencia de la edad fijada por cada red social, hay que tener en cuenta que se aplicará en nuestro país la de 14 años, como mínimo, si la que fija la red social es menor.

RED SOCIAL	AÑO DE CREACIÓN	FUNDADORES	CARACTERÍSTICAS	EDAD MÍNIMA DE ACCESO
LINKEDIN	2002	Reid Hoffman	Permite el contacto entre profesionales y empresas.	16 años
FACEBOOK	2004	Mark Zuckerberg	Da soporte para crear y compartir contenidos (imágenes, texto, vídeo).	13 años
YOUTUBE	2005	Steve Chen, Chad Hurley y Jawed Karim	Permite visualizar, crear y compartir vídeos online.	13 años

X (TWITTER)	2006	Evan Williams y Biz Stone, con la colaboración de Jack Dorsey y Noah Glass	Da soporte para crear y compartir cualquier tipo de información con un formato máximo de 280 caracteres.	13 años
WHATSAPP	2009	Jan Koum	Comenzó como una aplicación de mensajería, te permite enviar archivos de toda clase (textos, imágenes, vídeos y también documentos, así como ubicación, etc.).	13 años
INSTAGRAM	2010	Kevin Systrom y Mike Krieger	Permite a los usuarios subir y compartir imágenes y vídeos.	14 años
TWITCH	2011	Justin Kan y Emmet Shear	Permite la transmisión en vivo de vídeos.	13 años
TIKTOK	2016	Procedencia China, nombre original “Douyin”)	Da soporte para crear y compartir vídeos cortos de un máximo de 1 minuto de duración.	13 años

A continuación, se detallan diferentes características bajo las que se pueden clasificar las redes sociales:

- **Según la finalidad**. Se clasifican teniendo en cuenta el uso que le darán los usuarios. Las categorías son:

  - **Ocio**. Su principal finalidad es crear y reforzar relaciones personales. Se centran en la interacción entre usuarios a través de imágenes, textos, vídeos y/o comentarios, además de facilitar la comunicación privada a través de mensajes sólo accesibles entre pares, (por ejemplo, Instagram).
  - **Uso profesional**. Su fin es facilitar a los usuarios promocionarse a nivel profesional, estar actualizado sobre novedades de empleo y aumentar sus contactos profesionales. (Ej. LinkedIn).

Se debe tener claro que una misma red social puede ser usada con diferentes finalidades dependiendo de los objetivos del usuario. Por ejemplo, en Instagram puede haber usuarios cuya finalidad sea el ocio y otros para los que sea su medio de trabajo, por ejemplo, los *influencer*. Dependiendo de la finalidad, las recomendaciones de seguridad y privacidad variarán. Mientras la finalidad sea el ocio, por ejemplo, se recomendará mantener los perfiles privados; en el caso de ser para uso profesional, esta medida no tendrá mucho sentido puesto que nadie tendría acceso a ver lo que se promociona.

- **Según el modo de funcionamiento**. Se considera la estructura y las acciones que permite realizar la red social, según la forma en la que está configurada y restringida. Se divide en las siguientes categorías:

  - **Contenidos**. Los usuarios crean y comparten contenidos en soporte escrito y/o audiovisual con otros usuarios. Normalmente, en este tipo de redes sociales, los perfiles son públicos y no se limita la información a usuarios registrados o a los contactos. (Ej. YouTube).
  - **Basado en perfiles**: Estos pueden ser de carácter personal o profesional. Consisten en fichas donde los usuarios incorporan información personal o profesional, que suelen ir acompañadas de fotografías. En este tipo de redes sociales, tenemos obligatoriamente que crear un perfil para poder hacer uso de la red social.

- ***Microblogging***. La información que se puede compartir en estas redes suele estar limitada a contenidos breves o incluso limitarlo a ciertos números de caracteres. Persiguen crear dinamismo en la utilización, facilitar que sus contenidos sean emitidos y consumidos desde dispositivos móviles y que los usuarios realicen un seguimiento continuo de los mismos. En ocasiones, también son conocidos con el nombre de *nanoblogging*. (Ej. X, antes Twitter).

➢ **Según el nivel de apertura**. Se clasifican en base a la capacidad de acceso de los usuarios y el nivel de restricciones que se aplican.

- **Accesibles**. Están accesibles y pueden ser utilizadas por cualquier persona que cuente con acceso a Internet. Es decir, no están restringidos a un grupo, colectivo u organización especifica. (Ej. YouTube, SnapShat).
- **Restringidas**. Solo se puede acceder a ellas si se pertenece a un colectivo específico u organización privada. Los usuarios pueden llegar a necesitar una licencia o relación contractual de otra índole para poder utilizarlas. (Ej. Yammer).

➢ **Según el nivel de integración**. Se clasifican en base al nivel de afinidad e intereses de los usuarios y actividades que realizan en ellas (Ej. educativo/profesional).

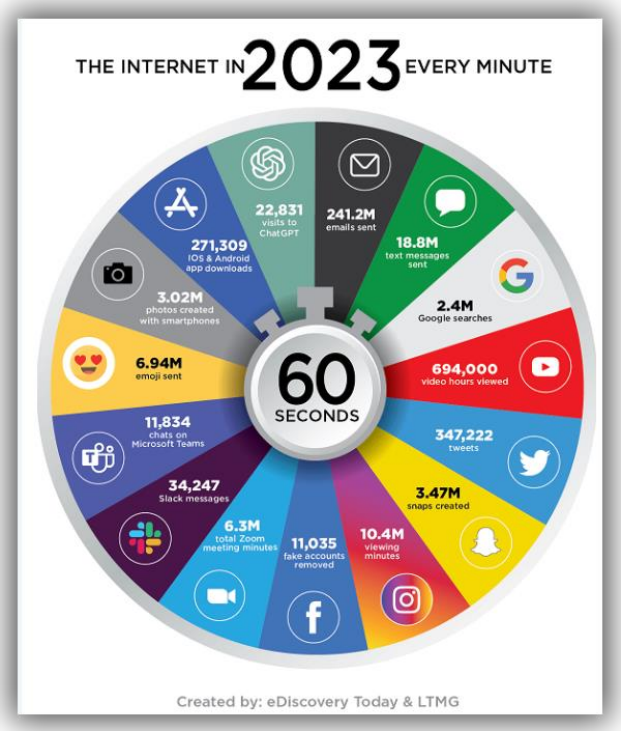
- **Vertical**. Los usuarios de la red social se adhieren a ella alrededor de un tema específico. El interés común puede ser formativo, una temática concreta o pertenencia profesional. En ocasiones el usuario debe disponer de una invitación previa por parte de uno de sus miembros para poder acceder. (ej. TripAdvisor, Moodle).
- **Horizontal.** El uso de la red no está limitado a algo concreto, los usuarios pueden tener intereses de todo tipo. (ej. Facebook, WhatsApp).

En la tabla podemos ver un análisis de las principales redes sociales, en cuanto su finalidad, funcionamiento, grado de apertura e integración. Existen una serie de aspectos comunes, por ejemplo, todas son públicas y su integración es de carácter horizontal, esta última se define como una estrategia de las redes sociales para ofrecer sus servicios a diferentes mercados.

		YouTube	Facebook	Instagram	X (Twitter)	LinkedIn	TikTok	Twitch	WhatsApp
FINALIDAD	Ocio	X	X	X	X	X	X	X	X
	Uso profesional	X	X		X	X			X
FUNCIONAMIENTO	Contenidos	X			X		X	X	
	Basados en perfiles	X	X	X	X	X			X
	Microblogging				X				
GRADO DE APERTURA	Accesibles	X	X	X	X	X	X	X	X
	Restringidas								
INTEGRACIÓN	Vertical								
	Horizontal	X	X	X	X	X	X	X	X

Algo interesante es que la mayoría de las redes sociales tienen una finalidad de ocio, pese a que se puedan utilizar en perfiles profesionales, excepto redes sociales del tipo LinkedIn, cuya finalidad principal es la profesional. Otro aspecto a destacar es la diferencia en el funcionamiento, algunas redes sociales se basan en contenidos, como el caso de Tiktok, otras solo en perfiles, como el caso de LinkedIn y en cambio otras se basan en ambos, contenidos y perfiles, como puede ser Facebook.

En la siguiente infografía podrás conocer qué pasaba en Internet, en las diferentes redes sociales, en tan solo un minuto durante 2023:



2. ¿Por qué nos exponemos en redes sociales? ¿Cómo nos puede afectar?

Son varios los motivos que nos llevan a utilizar redes sociales, accedemos a ellas para **comunicar y compartir**. Las redes sociales son una plataforma ideal para el intercambio de información y exposición de opiniones. También son una forma para **mantener o establecer contacto,** ya que permiten comunicarnos con nuestros seres queridos, buscar nuevas compañías, pareja, y fortalecer las relaciones profesionales. Por otro lado, nos pueden servir para estar **informados;** el volumen de información a nuestra disposición no tiene límites y podemos estar actualizados sobre cualquier acontecimiento en tiempo real. También podemos utilizar las redes sociales simplemente para **entretenernos** o incluso los usuarios más avanzados pueden utilizar estas plataformas para publicitarse. Cada vez más los usuarios siguen a los negocios que son de su agrado y establecen con ellos relaciones comerciales.

Por tanto, son muchos los beneficios que se desprenden de utilizar redes sociales, pero también debemos tener precaución con los riesgos que pueden conllevar. Hay que tener en cuenta que toda la información que compartimos en Internet y en las redes sociales, aunque posteriormente queramos eliminarla, ya habrá dejado un rastro y, además, alguien que la haya visualizado, la habrá podido copiar y/o difundir.

A continuación, se enumeran algunos ejemplos de tipos de información cuyas publicaciones pueden derivar en efectos negativos y tener consecuencias no deseadas:

- **Correo electrónico y número de teléfono:** Si los hacemos públicos, corremos el riesgo de ser víctimas de *spam*, *phishing* o cualquier tipo de ataque con métodos de ingeniería social.
- **Dirección y ubicación en tiempo real**: Si exponemos dónde nos encontramos, qué lugares frecuentamos y cuándo no estamos en casa puede llegar a ser muy peligroso. Un ejemplo muy conocido es el de los recientes robos en casas de futbolistas. En este enlace encontrarás más sobre el peligro de compartir estos datos: Ver enlace
- **Fotos o vídeos de menores**: Cuando compartimos fotos de menores, tenemos que ser cautelosos porque no sabemos a dónde pueden llegar y quién tendrá acceso a ellas, lo mejor es siempre tapar el rostro.
- **Fotos inapropiadas**: Es el caso de las fotos o imágenes comprometidas o de carácter sexual. Su difusión afecta directamente a nuestra identidad y

debemos reflexionar siempre antes de hacerlo, ya que podría derivar en consecuencias como la sextorsión o el ciberacoso.

- **Publicaciones ofensivas o comentarios comprometidos**: Cuando nos expresemos en Internet siempre deberemos hacerlo cumpliendo unas normas de netiqueta. Comentarios inapropiados pueden llegar a afectar a terceros y/o perjudicarnos personal o profesionalmente. Además, insultar o amenazar en las redes es un delito al igual que hacerlo presencialmente.
- **Documentos personales**: Debemos tener cuidado de no revelar nuestros datos personales sensibles, como el DNI, datos bancarios o cualquier otra información delicada que pueda ser utilizada para suplantar nuestra identidad o realizarnos algún ataque mediante ingeniería social.
- **Conversaciones privadas**: Al igual que no debemos compartir fotos de terceros sin su consentimiento, las conversaciones privadas no deben ser expuestas si la otra persona no está de acuerdo.

2.1 Consecuencias de una sobreexposición

A continuación, expondremos las principales consecuencias que pueden derivarse de una sobreexposición en las redes sociales:

- **Suplantación de identidad:** Si hacemos una sobreexposición de nuestra información, los ciberdelincuentes podrán llegar a crearse perfiles en redes sociales que suplanten nuestra identidad, y con ellos realizar algún tipo de fraude o perjudicar nuestra identidad digital.
- **Ataques de ingeniería social:** Los ciberdelincuentes pueden recopilar toda la información que encuentren sobre nosotros y perfeccionar sus ataques de ingeniería social según nuestras características e intereses, haciendo que sus fraudes tengan más credibilidad ante nuestros ojos y sean más difíciles de detectar.
- **Riesgo de rastreo:** Al hacer pública nuestra ubicación y movimientos, podemos exponer nuestra seguridad física ante ataques fuera del mundo digital.
- **Reputación *online*:** Si exponemos información, datos u opiniones sensibles, estos podrían afectar a nuestra reputación online, ahora o en el futuro.

¿Qué precauciones debemos tomar a la hora de publicar en redes sociales?:

- **Configurar las opciones de privacidad y seguridad.** Donde podremos determinar, por ejemplo, qué personas podrán visualizar nuestras publicaciones.
- **Publicar lo estrictamente necesario:** Tener una sobreexposición en las redes sociales suele tener mayores inconvenientes que beneficios.
- **No compartir nunca información sensible:** Como hemos visto, nunca debemos exponer nuestro correo electrónico, número de teléfono, dirección, ubicación, fotografías o vídeos de otras personas y en especial de menores, fotografías íntimas o de carácter sexual, documentos personales, opiniones, quejas o comentarios comprometedores y conversaciones privadas.
- **Evitar entrar en discusiones con desconocidos:** Internet y en especial las redes sociales están plagadas de troles o *haters* que aprovechan la Red para fomentar el enfrentamiento entre usuarios. Esto puede derivar en situaciones desagradables que es mejor evitar.

3. Riesgos principales de redes sociales

Como hemos visto en módulos anteriores, las redes sociales son unas herramientas muy potentes con gran alcance y que nos ofrecen muchas ventajas, pero es importante ser conscientes de los **peligros que pueden ocasionar**. Por ello debemos saber identificarlos, cómo evitarlos y qué hacer en caso de ser víctimas.

Conozcamos los **principales riesgos que pueden entrañar las redes sociales**.

3.1 Suplantación de identidad

Es uno de los principales problemas relacionados con la privacidad a los que se enfrentan los usuarios de redes sociales. La suplantación de identidad consiste en que un ciberdelincuente se hace pasar por nosotros, para causarnos daño a nuestra reputación o poder llevar a cabo diferentes actividades ilícitas, como fraudes hacia nuestros contactos, para sustraer información personal o infección por *malware*.

El ciberdelincuente que tiene intención de suplantar una identidad recopila toda la información sobre su víctima para poder crear un perfil falso.

En ocasiones, se puede pensar que solo las personas conocidas, famosos o gente con alto poder adquisitivo pueden llegar a ser víctimas de suplantación de identidad, pero nada más lejos de la realidad. Cualquier usuario con presencia en la red corre el riesgo de que su identidad sea suplantada y, de hecho, durante los últimos años se ha incrementado el número de suplantaciones de identidad en las redes sociales.

¿Cómo protegernos?

Para prevenir la suplantación de identidad debemos seguir las **buenas prácticas de uso** de las redes sociales protegiendo, así, nuestra privacidad. Además de tener las configuraciones de seguridad y privacidad oportunas como, por ejemplo, tener activado el doble factor de autenticación (que desarrollaremos a continuación), debemos compartir solo la información necesaria, tratando con especial cuidado los datos sensibles como el DNI, email, dirección, datos de autentificación, datos bancarios y también la información personal comprometida (como fotos, ubicaciones, gustos, etc.). También debemos usar el sentido común y sospechar de publicaciones, anuncios o solicitudes de amistad/contacto de desconocidos, así como evitar acceder o aceptar aquellas que nos generen sospecha.

¿Qué hacer en caso de ser víctima?

En caso de ser víctima de una suplantación de identidad, lo primero que se recomienda es contactar con el **Centro de Ayuda de la red social** en la que se ha producido la infracción para que tome las medidas oportunas. Además, en caso necesario, la víctima puede poner una denuncia por suplantación de la identidad ante las Fuerzas y Cuerpos de Seguridad del Estado, para lo que será necesario aportar todas las pruebas de las que se disponga, como capturas, imágenes o conversaciones que muestren el delito. También se puede acudir a la **Agencia Española de Protección de Datos**, aportando las pruebas mencionadas anteriormente.

MÁS INFORMACIÓN

Puedes ampliar la información sobre la forma de actuar tras una suplantación de identidad en el siguiente enlace.

3.2 Robo de cuentas

El robo de cuentas consiste en sustraer las credenciales de acceso a las redes sociales mediante el uso de técnicas de **ingeniería social** o a través del ataque directo a nuestras contraseñas. En cuanto a las técnicas de ingeniería social, la más común es recibir un correo electrónico fraudulento donde los ciberdelincuentes se hacen pasar por la red social y nos informan de que debemos hacer clic en un enlace para verificar nuestro perfil. Al entrar veremos una web casi idéntica a la real pero que resulta ser falsa. En el caso de introducir nuestras credenciales, se las habremos facilitado a los ciberdelincuente, por lo que podrán acceder a nuestro perfil y cambiar los datos de acceso para que no podamos volver a entrar y tener control total sobre nuestra cuenta. Otra forma de robar nuestras contraseñas es utilizando una técnica denominada "fuerza bruta", cuya metodología consiste en utilizar herramientas que prueban claves hasta dar con la correcta. Por esa razón es tan importante generar contraseñas robustas. Veremos esta cuestión en profundidad en el módulo "Gestión de contraseñas"

¿Cómo protegernos?

Para evitar que nos ocurra el robo de cuenta, existen diferentes formas de protegernos:

- Utilizar contraseñas robustas; con más de ocho caracteres y que contengan mayúsculas, minúsculas, caracteres especiales y números. Por ejemplo, M1redsicual11!
- No compartir las contraseñas con nadie.
- No reutilizar contraseñas en diferentes servicios.
- Utilizar mecanismos de protección adicionales, como la verificación en dos pasos.
- Evitar conectarse a las redes sociales desde dispositivos que no sean personales o los habituales. En caso de hacerlo, debemos cerrar siempre la sesión, eliminar los datos de la sesión y modificar la contraseña.

  Estar siempre atentos ante posibles fraudes y usar siempre el sentido común.

¿Qué hacer en caso de ser víctima?

En caso de ser víctima del robo de una cuenta de una red social, se debe denunciar ante la misma. Facebook, Instagram o X (Twitter) tienen mecanismos que te podrían permitir recuperar de nuevo tus credenciales. En caso necesario, deberán tomarse todas las pruebas y efectuar denuncia antes las Fuerzas y Cuerpos de Seguridad del Estado.

3.3 Contactos fraudulentos

Los contactos fraudulentos son aquellos que no son lo que dicen ser y que pueden ocasionarnos algún tipo de problema, por ejemplo, enviarnos enlaces maliciosos o archivos infectados con virus, divulgar *fake news,* es decir, noticias falsas o bulos, realizar publicaciones de carácter ofensivo o buscando discusión, o generarnos problemas de privacidad compartiendo nuestras publicaciones con malas intenciones.

¿Cómo identificarlos?

Tenemos que tener en cuenta una serie de aspectos para identificar este tipo de contactos:

- Si el perfil no tiene fotos publicadas, o muy pocas.
- Si las fotos que publica son demasiado profesionales para ser un perfil personal o bien parezcan tomadas de otras personas.
- Si la cuenta tiene poca interacción.
- Si los contactos, tanto seguidores como seguidos, no parecen verdaderos.

¿Cómo protegernos?

- Limpiar nuestra red social de contactos desconocidos y/o que consideremos sospechosos.
- Configurar la privacidad de nuestro perfil para evitar que nos envíen mensajes o etiqueten nuestras fotografías usuarios desconocidos.
- Comprobar los perfiles de los contactos que nos resulten sospechosos: si tienen descripciones pobres, fotografías o vídeos escasos o copiados de otra cuenta o sus publicaciones son siempre iguales y sospechosas (concursos, enlaces u otro tipo de fraudes)
- Hacer uso de las funciones de bloqueo y eliminación de usuarios que todas las redes sociales tienen.

¿Qué hacer en caso de detectarlo?

Las redes sociales tienen, en general, mecanismos que nos permiten denunciar aquellas cuentas que consideremos falsas. Por ejemplo, en Facebook, si entramos en un perfil sospechoso y pulsamos en denunciar, nos aparecen una serie de opciones, y una de ellas es denunciar “Cuenta falsa”.

3.4 Anuncios fraudulentos

En las redes sociales también existen anuncios publicitarios que facilitan que estos servicios sean gratuitos. Los ciberdelincuentes aprovechan esta casuística para incluir anuncios y publicaciones maliciosas que nos redirigen hacia páginas web fraudulentas. En caso de que accedamos al anuncio, terminarán solicitándonos información personal como los datos bancarios o infectando nuestro equipo con *malware*.

Estos anuncios aparecen en nuestras redes sociales utilizando una serie de técnicas que saltan los algoritmos que usan las redes sociales para comprobar los anuncios que se muestran.

¿Cómo identificarlo?

- Suelen ser anuncios demasiados atractivos y que presionan al usuario a comprar antes de que acabe la oferta.
- Suelen promocionar marcas reconocidas.
- Aunque la web simule la original, la URL no corresponde con la de la web real.
- Suelen tener una mala calidad tanto en la redacción como en las imágenes usadas.
- Escasa o nula información sobre la empresa y métodos de contacto.
- No se utilizan medios seguros de pago.

¿Cómo protegernos?

Existen diferentes maneras de protegernos:

- Añadir mecanismos de bloqueo de anuncios, mediante la configuración de la red social o instalando complementos en nuestro navegador.
- Analizar el contenido del anuncio, a través de posibles errores ortográficos o gramaticales en la redacción, las imágenes que contiene y el aviso legal.
- Comprobar comentarios y valoraciones que otros usuarios hayan dejado haciendo una búsqueda en Internet.
- Analizar la URL para comprobar si utiliza el protocolo seguro https, tiene certificado digital y el dominio coincide con el real de la entidad.

¿Qué hacer en caso de detectarlo o ser víctima?

En el caso de detectar un anuncio fraudulento, las plataformas de redes sociales suelen ofrecer una serie de mecanismos. En Facebook, por ejemplo, podemos pulsar en los tres puntos que se encuentran encima de cada publicación y hacer clic en “denunciar anuncio” y después indicar la causa de nuestra denuncia.

En el caso de ser víctima existen distintas posibilidades en función del supuesto del que se trate: acudir a la oficina de información del consumidor de tu municipio, reportar tu incidencia a INCIBE-CERT a través del email (incidencias@incibe-cert.es), también puedes contactar con la Línea de Ayuda de Ciberseguridad de INCIBE, llamando al 017, y denunciar el caso a las Fuerzas y Cuerpos de Seguridad del Estado.

3.4 Concursos fraudulentos

Uno de los procedimientos de promoción más habituales en las redes sociales son los sorteos o concursos. Los ciberdelincuentes también han encontrado en ellos un buen método para engañar a sus víctimas, por lo que debemos prestar especial atención a aquellos concursos que se nos muestran, ya que, en ocasiones, serán fraudulentos.

Estos anuncios contarán con un enlace en el que se solicitará información como nombre, correo electrónico, dirección y datos bancarios, que los ciberdelincuentes utilizarán para venderlos a terceros, utilizarlos en campañas de *spam* o, en el peor de los casos, para distribución de fraudes y *malware*.

¿Cómo protegernos?

Para protegernos de este tipo de fraude podemos seguir algunas recomendaciones:

- Realizar una búsqueda del concurso en otras fuentes como el canal web o los perfiles de redes sociales de la marca, para comprobar si realmente existe.
- Revisar si se facilitan bases legales y si estas son correctas. Ningún sorteo real se lleva a cabo sin bases legales.
- Analizar la URL para comprobar si utiliza https, tiene certificado digital y el dominio coincide con el real de la marca.
- Buscar comentarios que otros usuarios hayan dejado en Internet sobre el concurso y que pueden evidenciar su falsedad.
- Buscar fallos ortográficos y gramaticales. La mayoría de fraudes o promociones de dudosa reputación usan traductores para la creación del contenido.
- Contrastar las imágenes para comprobar que no sean sacadas de Internet, de mala calidad o copias de otros fraudes y/o concursos. Google, por ejemplo, permite comprobar si la imagen es una copia y su procedencia desde su buscador de imágenes: https://images.google.com.

- Además, si encontramos algún concurso fraudulento, podemos denunciarlo a la red social, para que eliminen su publicación y evitar que otros usuarios caigan en la trampa.

¿Qué hacer en caso detectarlo o ser víctima?

Tanto si detectamos un concurso fraudulento como si somos víctimas seguiríamos los mismos pasos que hemos visto en el apartado de anuncios fraudulentos.

3.5 *Fake news* o noticias falsas

Las redes sociales se han convertido en un medio donde proliferan las noticias falsas también conocidas como *fake news*. Su objetivo es causar alarma, desinformación, desconfianza entre las personas, y atacar o desprestigiar a personas o empresas.

¿Cómo protegernos?

- Contrastar la información, sobre todo antes de compartirla, buscando las fuentes o referencias de la noticia.
- Revisar la URL en la que se encuentra la noticia, para analizar si dispone de un certificado de seguridad y empieza por https. Esta medida por sí sola no es suficiente para identificar webs fiables, ya que los ciberdelincuentes más detallistas podrían adquirir este certificado pagando.
- Analizar el titular de la noticia, ya que en ocasiones suele tener un carácter sensacionalista. Además, es común que las noticias falsas utilicen titulares que luego no tienen nada que ver con su contenido o lo tergiversan.
- Comprobar el formato de la noticia, a veces se identifica fácilmente que es falsa, buscando errores ortográficos, traducciones mal hechas, imágenes de poca calidad o incluso robadas de otros sitios.

¿Qué hacer en caso detectarlo?

Si nos encontramos con una noticia falsa, no deberemos reenviarla ni interactuar, evitando así su difusión y propagación. Además, como hemos comentado en puntos anteriores, las propias redes sociales tienen mecanismos que nos ofrecen la posibilidad de denunciar las noticias falsas.

Por continuar con el mismo ejemplo, Facebook, al pulsar en denunciar nos muestra la opción de indicar "información falsa".

En este enlace podrás encontrar distintos recursos para combatir y denunciar las informaciones falsas y los bulos:

Ver enlace

3.6 Ciberacoso

En el caso de que compartamos demasiada información personal sobre nosotros mismos en redes sociales, nos estaremos exponiendo y podremos acabar siendo víctimas, por ejemplo, de ciberacoso.

Las víctimas de **ciberacoso** se ven sometidas a insultos, amenazas o difamaciones a través de medios digitales, y estos se vuelven más peligrosos que el acoso en la vida real ya que tiene una mayor intensidad y puede llegar a realizarse 24x7.

Aunque en muchos casos se vinculan estas prácticas a los jóvenes, por ser un colectivo vulnerable y su gran exposición en las redes, hay todo tipo de víctimas de casos de ciberacoso en las redes, por lo que todos debemos protegernos.

¿Cómo protegernos?

Es importante establecer restricciones en nuestras redes sociales a través de las opciones de configuración de seguridad y privacidad, además de limitar la información que exponemos sobre nosotros mismos en Internet, así como mantener unas credenciales seguras a través de contraseñas robustas y activando el segundo factor de autenticación.

¿Qué hacer en caso de ser víctima?

En el caso de ser víctimas de ciberacoso, no debemos responder a provocaciones sino bloquear el perfil y denunciarlo ante la red social. En caso necesario también podremos realizar una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado presentando todas las pruebas que tengamos del ciberacoso, como conversaciones, publicaciones online, etc.

En este enlace encontrarás diferentes recursos relacionados con el ciberacoso:

Ver enlace

3.7 Sextorsión

En este tipo de fraude se chantajea a la víctima a través de correos electrónicos o mensajes solicitando dinero o contenido sexual a cambio de no divulgar supuestas fotografías o vídeos íntimos en los que aparece la víctima.
No siempre requiere que se haya tenido contacto previo con un ciberdelincuente, ni siquiera que se haya enviado este tipo de contenidos a nadie. A veces, nos pueden llegar este tipo de correos o mensajes donde el ciberdelincuente asegurará disponer de este material, argumentando que tiene acceso a nuestra cámara web, por ejemplo, aunque realmente no está en posesión de ninguna fotografía o vídeo.

¿Cómo protegernos?

Para protegernos de ser víctimas de sextorsión debemos seguir estas recomendaciones:

- No revelar información personal a desconocidos, ni siquiera si creemos tener una relación especial con esta persona. Si no estamos seguros al cien por cien de sus intenciones, debemos evitar compartir fotografías, vídeos o información sensible sobre nosotros que pueda usarse en la sextorsión.
- Investigar a los usuarios nos ayudará a descartar a potenciales ciberdelincuentes. Por ejemplo, revisando sus perfiles, buscando su nombre de usuario o correo electrónico en Internet para ver si está registrado en más plataformas o está vinculado a algún fraude, etc.
- En el caso de que nos soliciten dinero, no enviarlo, ya que realizar el pago no garantiza que no nos sigan extorsionando.
- Evitar descargar archivos o entrar en enlaces sospechosos, ya que los correos fraudulentos y las webs no fiables son una de las principales causas de infección por *malware*. Los *spyware* son un tipo de *malware* especializado en hacer capturas y vídeos a través de webcams sin nuestro consentimiento.

¿Qué hacer en caso de ser víctima?

El primer paso será bloquear el contacto que nos está sextorsionando y denunciarlo ante la red social. En caso necesario se podrá denunciar ante las Fuerzas y Cuerpos de Seguridad del Estado aportando todas las pruebas que tengamos, como copia de las conversaciones mantenidas.

En este enlace encontrarás más información sobre la sextorsión:

Ver enlace