



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Taller “Riesgos y fraudes en redes sociales y protección de nuestra identidad digital”



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



TU AYUDA EN
CIBERSEGURIDAD




Oficina
de Seguridad
del Internauta

- ❖ 1. Redes sociales y nuestra identidad digital
- ❖ 2. Buenas prácticas al utilizar las redes sociales
- ❖ 3. Fraudes comunes en redes sociales



INTRODUCCIÓN

Las plataformas de redes sociales **almacenan una inmensa cantidad de información personal** que, si no tenemos cuidado, puede terminar en malas manos y exponer nuestra privacidad.

Por eso, es fundamental que aprendamos las **buenas prácticas vinculadas al uso de redes sociales**.



1. REDES SOCIALES Y NUESTRA IDENTIDAD DIGITAL



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD

A medida que avanza la tecnología y los usuarios pasamos más tiempo conectados a la Red, las aplicaciones y plataformas como las redes sociales también evolucionan, **pasando a definir nuestra identidad digital.**



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

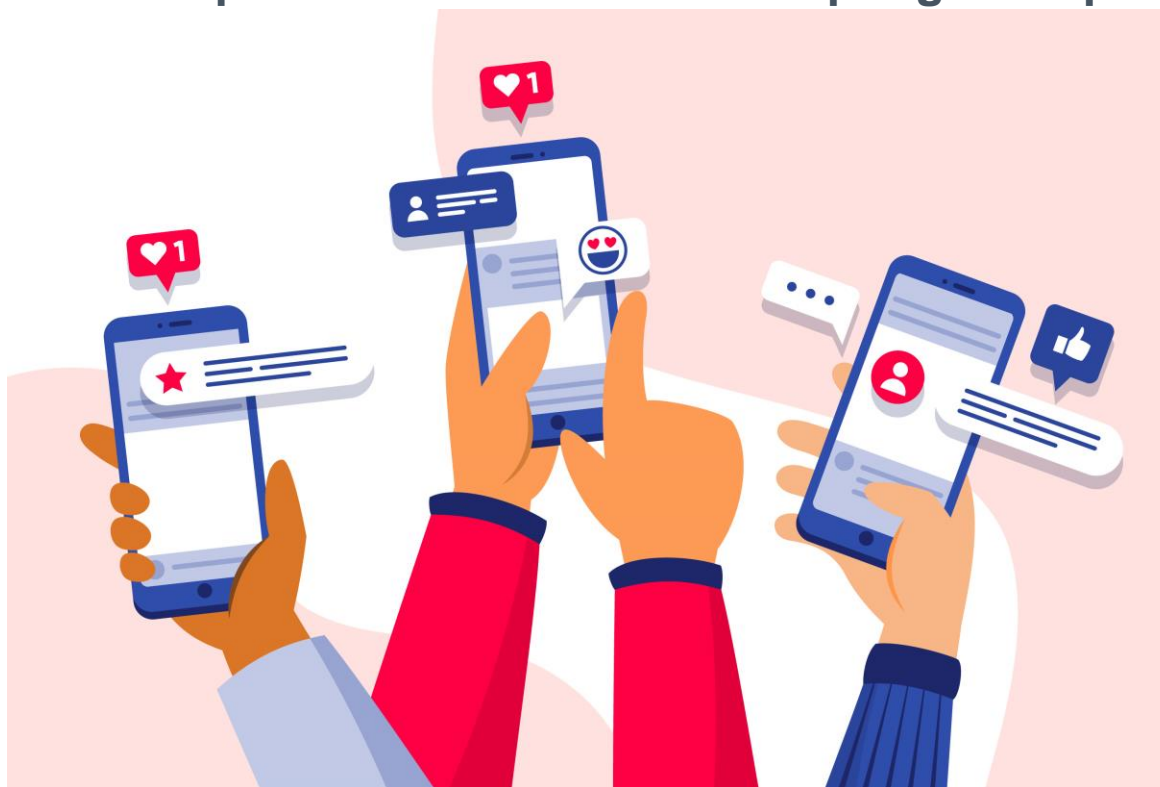
SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Cuando publicamos una foto, contestamos un comentario o subimos cualquier publicación a nuestras redes **estamos exponiendo parte de nosotros a la Red.**

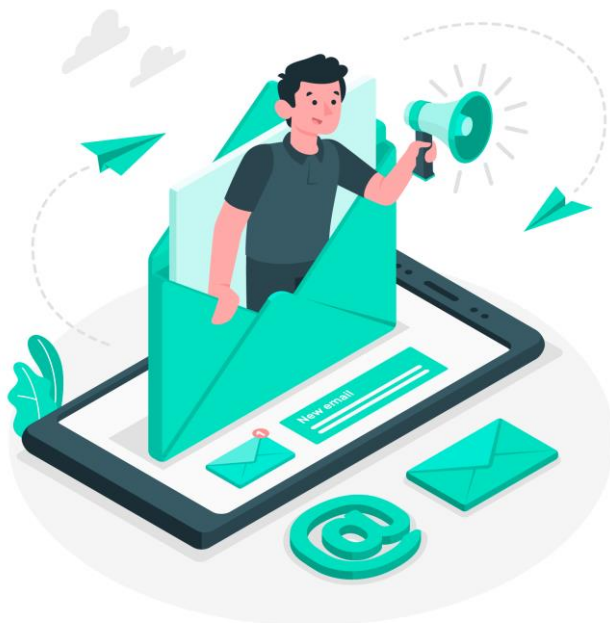
Es nuestra responsabilidad **controlar que estas interacciones no pongan en peligro nuestra privacidad.**



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. EVITAR COMPARTIR CIERTA INFORMACIÓN

Para evitar comprometer nuestra privacidad, es recomendable que **evitemos publicar o exponer la siguiente información en nuestras publicaciones, o en Internet:**

Correo electrónico

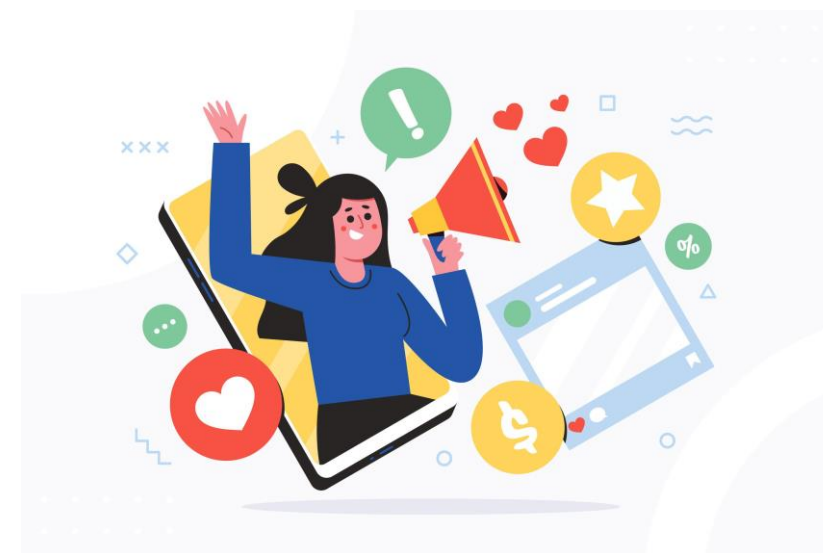


Número de teléfono



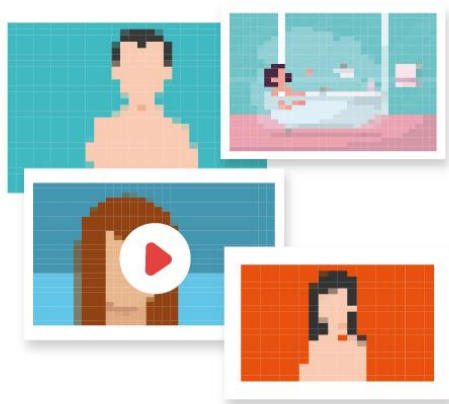
Dirección y ubicación

Fotografías / Vídeos de otras personas



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. EVITAR COMPARTIR CIERTA INFORMACIÓN

**Fotografías íntimas o
de carácter sexual**



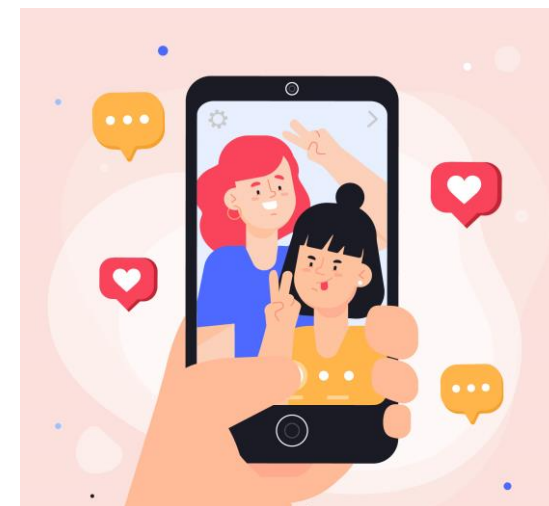
**Documentos
personales**



**Opiniones, quejas o
comentarios comprometedores**



**Conversaciones
privadas**



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD

La gran mayoría de redes sociales pone a disposición de sus usuarios diferentes **opciones de configuración** con las que modificar la seguridad de nuestra cuenta y limitar la cantidad de información que publicamos de forma abierta al resto de usuarios.

Facebook



Instagram



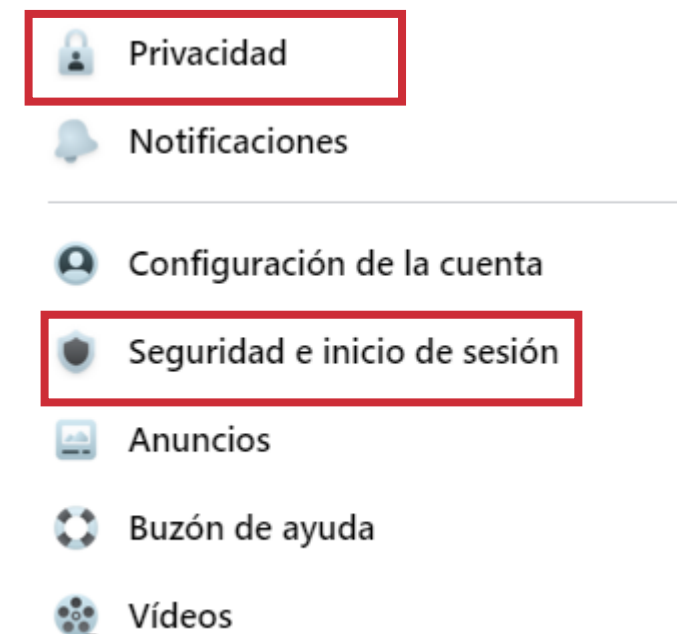
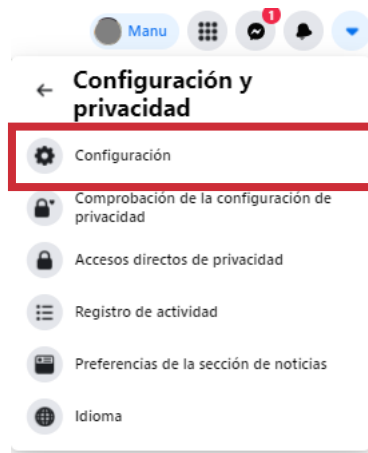
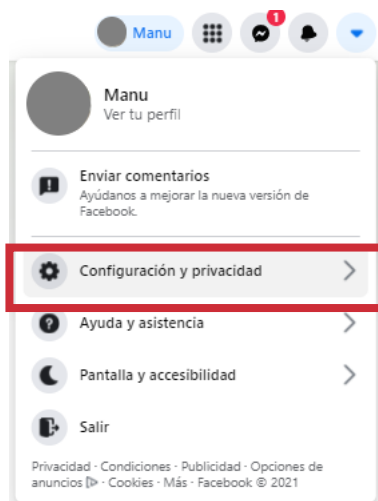
Twitter



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD: FACEBOOK

Para acceder a la configuración en **Facebook** deberemos:

- Hacer clic sobre el icono de flecha de la parte superior derecha y hacer clic en '**Configuración y privacidad**'. Luego, pulsaremos en '**Configuración**' para acceder al menú completo.













2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD: FACEBOOK

En ‘**Seguridad e inicio de sesión**’, accederemos a las opciones de seguridad:

1. **Dónde has iniciado sesión:** para comprobar los dispositivos dónde hemos iniciado sesión.
2. **Inicio de sesión:** para cambiar nuestra contraseña.
3. **Autenticación en dos pasos:** para añadir un paso adicional al iniciar sesión.
4. **Configurar la seguridad adicional:** para activar alertas en caso de inicios de sesión sospechosos.

Seguridad e inicio de sesión

Recomendado	
 Comprueba tus opciones de seguridad importantes Te indicaremos algunos pasos que te ayudarán a proteger tu cuenta.	Ver
Dónde has iniciado sesión	
 Ordenador Windows · Madrid, Spain Chrome · Activa ahora	
 Xiaomi Mi 9T · Madrid, Spain Aplicación de Facebook · hace 22 horas	
Ver más	
Inicio de sesión	
 Cambiar contraseña Se recomienda usar una contraseña segura que no uses para ningún otro sitio.	Editar
 Guardar información de inicio de sesión Activado · Solo se guardará en los navegadores y dispositivos que elijas.	Editar
Autenticación en dos pasos	
 Usar la autenticación en dos pasos Te pediremos un código si detectamos un intento de inicio de sesión desde un dispositivo o navegador no reconocido.	Editar
 Inicios de sesión autorizados Consulta una lista de los dispositivos en los que no es necesario que utilices un código de inicio de sesión.	Ver
 Contraseñas de aplicaciones Usa contraseñas especiales para iniciar sesión en tus aplicaciones en lugar de usar tus contraseñas o códigos de inicio de sesión de Facebook.	Añadir
Configurar seguridad adicional	
 Recibir alertas sobre inicios de sesión no reconocidos Te informaremos en caso de que alguien entre desde un dispositivo o un navegador que no usas habitualmente.	Editar
 Elegir entre tres y cinco amigos con los que ponerte en contacto si pierdes el acceso a tu cuenta Tus contactos de confianza pueden enviarte un código y una URL de Facebook para ayudarte a iniciar sesión.	Editar

2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD: FACEBOOK

En ‘Privacidad’ podremos modificar algunas opciones sobre lo que otros pueden ver de nosotros, como:

1. **Tu actividad:** para decidir quién puede ver nuestras publicaciones.
2. **Cómo pueden encontrarte y ponerse en contacto contigo las personas:** para decidir el tipo de interacción que otros usuarios pueden tener con nosotros.



Configuración y herramientas de privacidad

Accesos directos de privacidad	Comprobar algunas opciones importantes de la configuración Revisa rápidamente algunas opciones importantes de la configuración para asegurarte de que compartes el contenido con las personas que quieres.		
	Administrar tu perfil Ve a tu perfil para cambiar la privacidad de tu información, como quién puede ver tu cumpleaños o tus relaciones.		
	Consultar los aspectos básicos de la privacidad para obtener más información Obtén respuestas a preguntas frecuentes con esta guía interactiva.		
Tu actividad	¿Quién puede ver las publicaciones que hagas a partir de ahora?	Amigos	Editar
	Revisa todas tus publicaciones y los contenidos en los que se te ha etiquetado		Usar registro de actividad
	¿Quieres limitar la audiencia de las publicaciones que has compartido con los amigos de tus amigos o que has hecho públicas?		Limitar la audiencia de publicaciones anteriores
Cómo pueden encontrarte y ponerse en contacto contigo las personas	¿Quién puede ver las personas, páginas y listas que sigues?	Amigos	Editar
	¿Quién puede enviarte solicitudes de amistad?	Todos	Editar
	¿Quién puede ver tu lista de amigos?	Público	Editar
	¿Quién puede buscarte con la dirección de correo electrónico que has proporcionado?	Todos	Editar
	¿Quién puede buscarte con el número de teléfono que has proporcionado?	Todos	Editar
	¿Quieres que los motores de búsqueda fuera de Facebook enlacen a tu perfil?	Sí	Editar

2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD: FACEBOOK

En **‘Perfil y etiquetado’** también podremos limitar el tipo de información que está accesible para otros usuarios:

1. **Ver y compartir:** para decidir si queremos que otros usuarios publiquen en nuestro muro.
2. **Etiquetar:** para impedir que desconocidos nos etiqueten.
3. **Revisar:** para filtrar publicaciones donde nos quieran etiquetar.

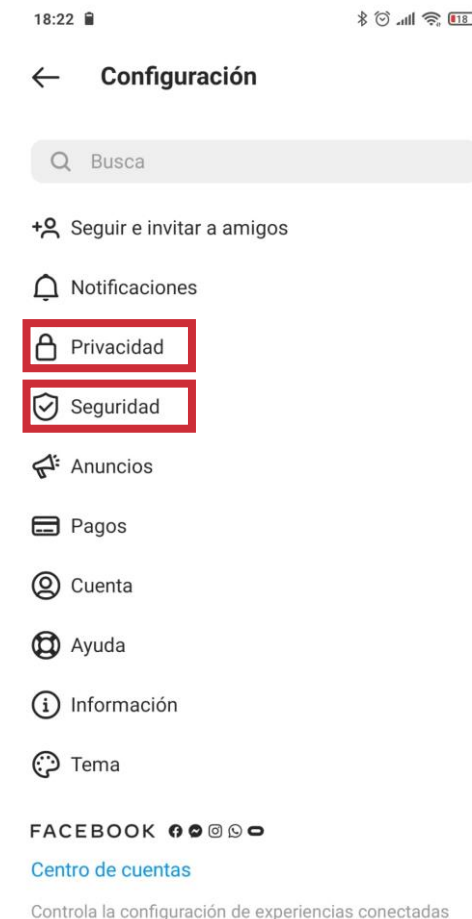
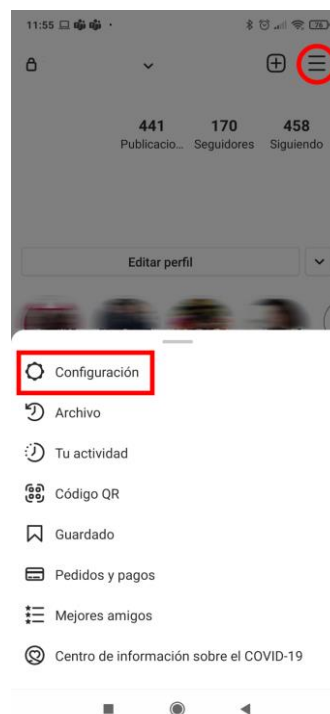
Perfil y etiquetado

Ver y compartir	¿Quién puede publicar en tu perfil?	Amigos	Editar
	Quién puede ver lo que otros publican en tu perfil	Amigos de amigos	Editar
	¿Permitir que otras personas compartan tus publicaciones en sus historias?	Activado	Editar
	Ocultar los comentarios que contengan ciertas palabras de tu perfil	Desactivado	Editar
Etiquetar	¿Quién puede ver las publicaciones en las que te ha etiquetado en tu perfil?	Amigos de amigos	Editar
	Cuando alguien te etiquete en una publicación, ¿a quién quieres añadir a la audiencia si aún no puede verla?	Amigos	Editar
Revisar	¿Revisar las publicaciones en las que se te etiquete antes de que aparezcan en tu perfil?	Activado	Editar
	Comprueba lo que ven otras personas en tu perfil		Ver como
	¿Quieres revisar las etiquetas que las personas añaden a tus publicaciones antes de que aparezcan en Facebook?	Desactivado	Editar

2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD: INSTAGRAM

Para acceder a la configuración de **Instagram** deberemos:

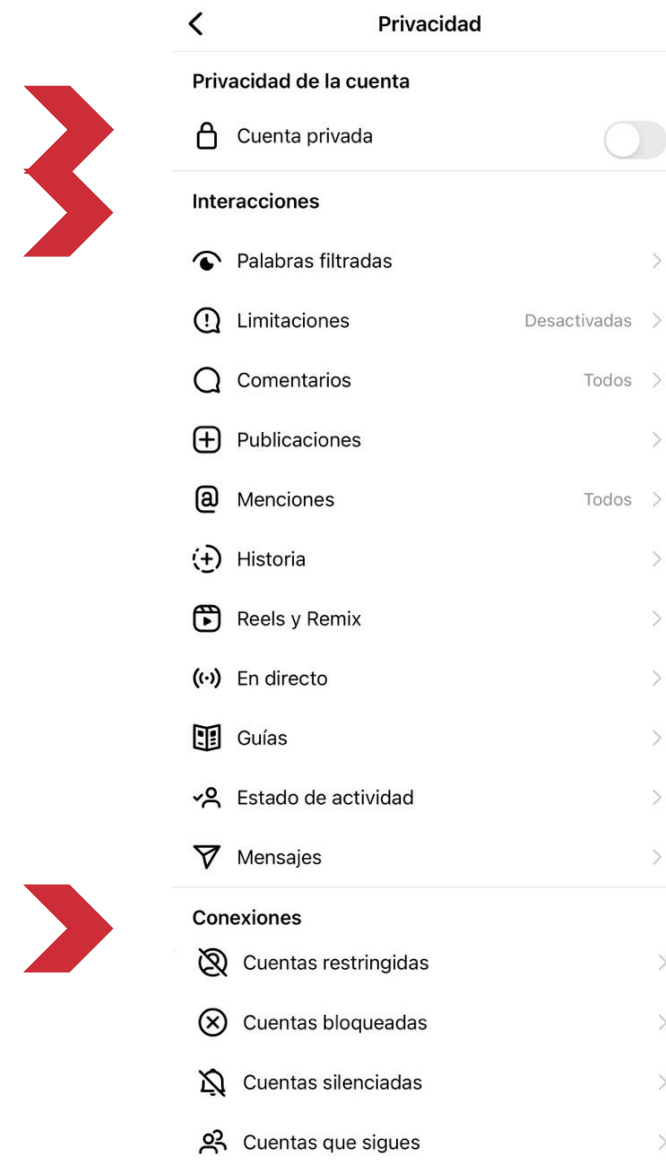
- Hacer clic sobre nuestra **foto de perfil** y luego pulsar en el **icono con las tres líneas** > '**Configuración**'. En el desplegable, encontraremos las diferentes opciones.



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD: INSTAGRAM

En 'Privacidad', podremos llevar a cabo diferentes ajustes:

1. **Cuenta privada:** para evitar que desconocidos vean nuestro perfil.
2. **Interacciones:** para configurar si otros usuarios pueden contactarnos.
3. **Conexiones:** para configurar las cuentas que tengamos bloqueadas.



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD: INSTAGRAM





Las opciones de '**Seguridad**' nos ayudarán a proteger mejor nuestra cuenta:

1. **Seguridad del inicio de sesión:** para cambiar la contraseña, comprobar los inicios de sesión, etc.
2. **Acceder a datos:** para comprobar todo lo que subimos a la red social.



< Seguridad	
Seguridad de inicio de sesión	
 Contraseña	>
 Actividad de inicio de sesión	>
 Información de inicio de sesión guardada	>
 Autenticación en dos pasos	>
 Correos electrónicos de Instagram	>
 Comprobación rápida de seguridad	>



Datos e historial	
 Acceder a datos	>
 Descargar datos	>
 Aplicaciones y sitios web	>
 Borrar historial de búsqueda	>

2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD: TWITTER

Para acceder a la configuración de **Twitter** deberemos:

- Pulsar sobre la foto de nuestro perfil y luego en '**Configuración y privacidad**'. Dentro de '**Privacidad y seguridad**' veremos varias opciones.



Tu cuenta

Consulta la información de tu cuenta, descarga un archivo con tus datos u obtén más información acerca de las opciones de desactivación de la cuenta.

Seguridad y acceso a la cuenta

Administra la seguridad de tu cuenta y lleva un control de su uso, incluidas las aplicaciones que conectaste a ella.

Monetización

Descubre cómo puedes ganar dinero en Twitter y administrar tus opciones de monetización.

Privacidad y seguridad

Administra qué información ves y compartes en Twitter.

Notificaciones

Selecciona los tipos de notificaciones que quieres recibir sobre tus actividades, intereses y recomendaciones.

Accesibilidad, pantalla e idiomas

Administra cómo ves el contenido de Twitter.

Recursos adicionales

Consulta otros lugares para obtener más información útil sobre los productos y servicios de Twitter.

2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONFIGURAR LAS OPCIONES DE PRIVACIDAD Y SEGURIDAD: TWITTER

1. **Audiencia y etiquetas:** proteger tweets y etiquetado de fotos.
2. **Tus tweets:** indicar si tu contenido multimedia es delicado.
3. **Contenido que ves:** según temas e intereses.
4. **Silenciar y bloquear:** configurar cuentas, palabras y notificaciones.
5. **Mensajes directos:** para evitar que desconocidos puedan enviarnos mensajes.
6. **Espacios:** configurar si los seguidores pueden ver que espacios escuchas.
7. **Visibilidad y contactos:** para evitar que puedan ver nuestro correo o teléfono.

Tu actividad en Twitter

-  **Audiencia y etiquetas**
 Administra qué información permites que vean otras personas en Twitter. >
-  **Tus Tweets**
 Administra la información asociada a tus Tweets. >
-  **Contenido que ves**
 Decide qué ver en Twitter en función de los temas e intereses de tu preferencia. >
-  **Silenciar y bloquear**
 Administra las cuentas, palabras y notificaciones que silenciaste o bloqueaste. >
-  **Mensajes directos**
 Administra quiénes pueden enviarte mensajes directamente. >
-  **Espacios**
 Administra quién puede ver la actividad de escucha de tus Espacios >
-  **Visibilidad y contactos**
 Controla tu configuración de visibilidad y administra los contactos que hayas importado. >

ACTIVIDAD 1



Por muy concienciados que estemos, siempre podemos cometer un error o despistarnos.

Para evitarlo, es conveniente que configuremos nuestras redes sociales de modo que estén lo más protegidas posibles contra fugas de información, protección de nuestras cuentas y para limitar la visibilidad de nuestro perfil.

Dedica unos minutos para configurar correctamente tu red social favorita.

2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. CONTROLAR NUESTRO CÍRCULO DE CONTACTOS

Cada uno es libre de agregar y comunicarse con quien quiera, pero **debemos saber que agregar contactos desconocidos puede ser peligroso para nuestra privacidad:**

1. Pueden buscar usuarios que publiquen demasiada información personal para robarla o suplantar su identidad.
2. Cuentas falsas o 'bots' que compartan enlaces maliciosos o *malware*.
3. Usuarios que publiquen contenido inapropiado, conflictivo o que dañe nuestra identidad digital.
4. Usuarios que saquen capturas de nuestras publicaciones.



designed by freepik

© 2006 The Authors
Journal compilation © 2006 Blackwell Publishing Ltd

Debemos tener **control sobre nuestros contactos, intentando limitarlo únicamente a aquellos usuarios que conocamos** o, en su defecto, que hayamos podido investigar lo suficiente como para descartar los ejemplos anteriores.



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. DESCARGAR NUESTRA VIDA DE LAS REDES SOCIALES

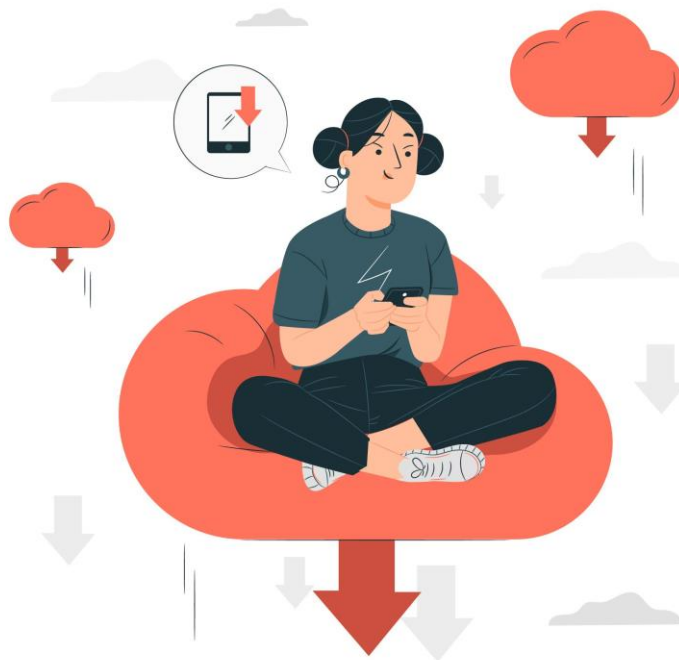


VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



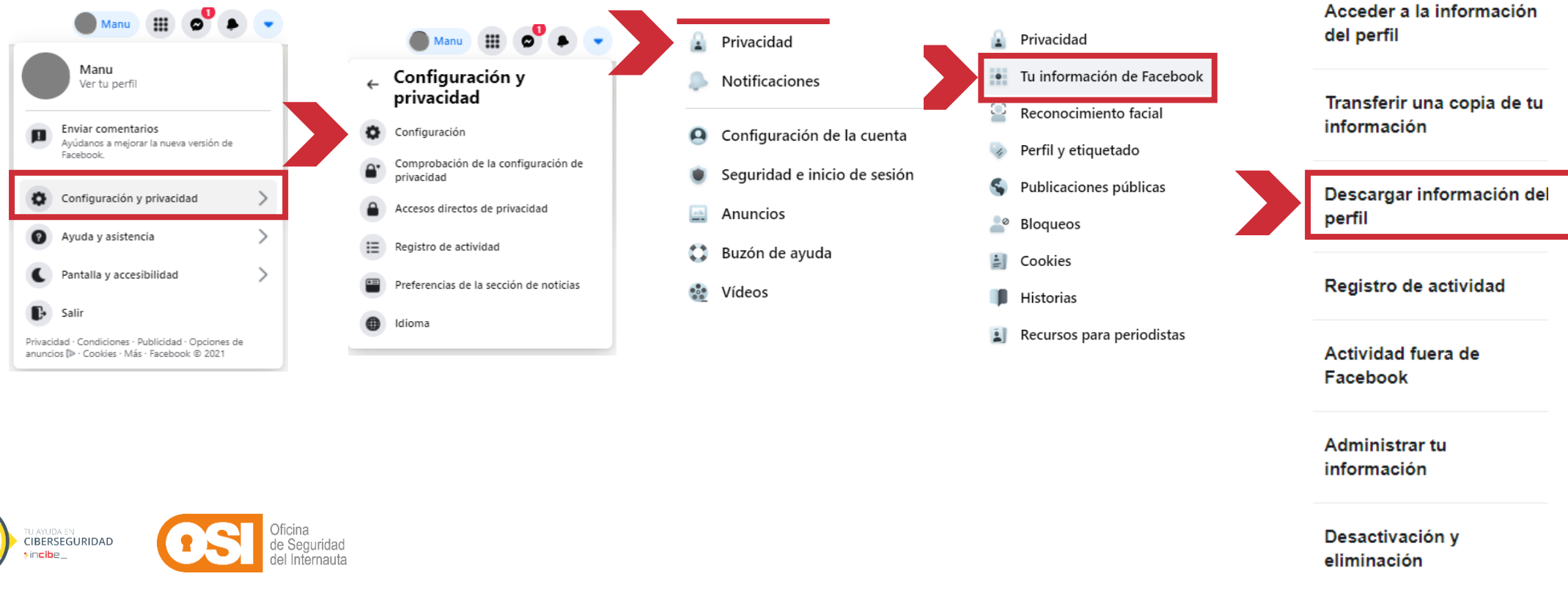
Con el uso, las redes sociales almacenan una gran cantidad de información sobre nosotros y nuestras interacciones, llegando a conformar toda una vida en este tipo de plataformas. Para tener visibilidad, **podemos descargar todos los datos almacenados sobre nosotros.**



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. DESCARGAR NUESTRA VIDA DE LAS REDES SOCIALES. FACEBOOK

En Facebook, podemos descargar una copia de nuestros datos desde su aplicación móvil o a través de la web. Para ello, seguiremos los siguientes pasos:

1. Accederemos a **'Configuración y privacidad' > 'Configuración' > 'Privacidad' > 'Tu información de Facebook' > 'Descargar información del perfil'**.



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. DESCARGAR NUESTRA VIDA DE LAS REDES SOCIALES. FACEBOOK

2. A continuación, podremos ‘añadir o eliminar categorías de datos a tu solicitud’, personalizando el contenido a descargar.

3. Una vez personalizado y configurado las opciones de la solicitud, seleccionaremos ‘**Crear archivo**’ para confirmarlo.

Seleccionar opciones de archivo

Puedes elegir el formato de archivo, la calidad del contenido multimedia y el intervalo de fechas de la descarga. El formato HTML favorece la visualización, mientras que el formato JSON permite a otro servicio importar el archivo más fácilmente. La calidad del contenido multimedia se refiere a la calidad de las fotos y los vídeos, y también afecta al tamaño del archivo.

Formato HTML	▼
Calidad del contenido multimedia Alta	▼
Intervalo de fechas (obligatorio) Últimos 3 años	▼

Tu actividad en Facebook ⓘ Desmarcar todo

	Elementos guardados y colecciones Lista de las publicaciones que has guardado y tu actividad en las colecciones	<input checked="" type="checkbox"/>
	Mensajes Mensajes que has intercambiado con otras personas en Messenger	<input checked="" type="checkbox"/>
	Publicaciones Publicaciones que has compartido en Facebook, publicaciones que has ocultado de tu biografía y encuestas que has creado	<input checked="" type="checkbox"/>
	Páginas Tus páginas, páginas que te han gustado o has recomendado, páginas que sigues y páginas que has dejado de seguir	<input checked="" type="checkbox"/>
	Encuestas Encuestas que has creado y en las que has participado	<input checked="" type="checkbox"/>
	Eventos Tus respuestas a eventos y una lista de los eventos que has creado	<input checked="" type="checkbox"/>
	Facebook Gaming Tu perfil de Facebook Gaming y juegos instantáneos a los que has jugado	<input checked="" type="checkbox"/>
	Tus lugares Lista de los lugares que has creado	<input checked="" type="checkbox"/>

2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. DESCARGAR NUESTRA VIDA DE LAS REDES SOCIALES. FACEBOOK

4. Finalmente, en **‘Configuración y privacidad’ > ‘Configuración’ > ‘Privacidad’ > ‘Tu información de Facebook’ > ‘Copias disponibles’** aparecerá el estado de nuestra solicitud como **‘Pendiente’**.

Tras unos días, aparecerá la opción para **‘Descargar’** toda nuestra vida en Facebook.

Información del perfil, Publicaciones, Me gusta y reacciones y más
Solicitado el 10 ene a las 17:29
Formato HTML
Archivos multimedia de calidad media

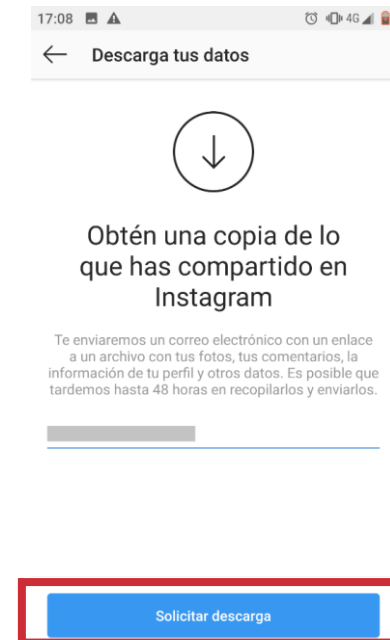
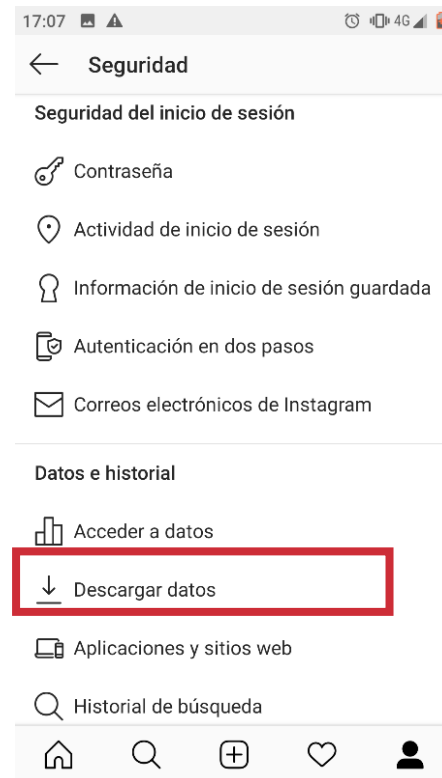
Pendiente

Cancelar

2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. DESCARGAR NUESTRA VIDA DE LAS REDES SOCIALES. INSTAGRAM

Instagram nos enviará un archivo en formato .zip con todos los datos de nuestra cuenta, siguiendo estos pasos:

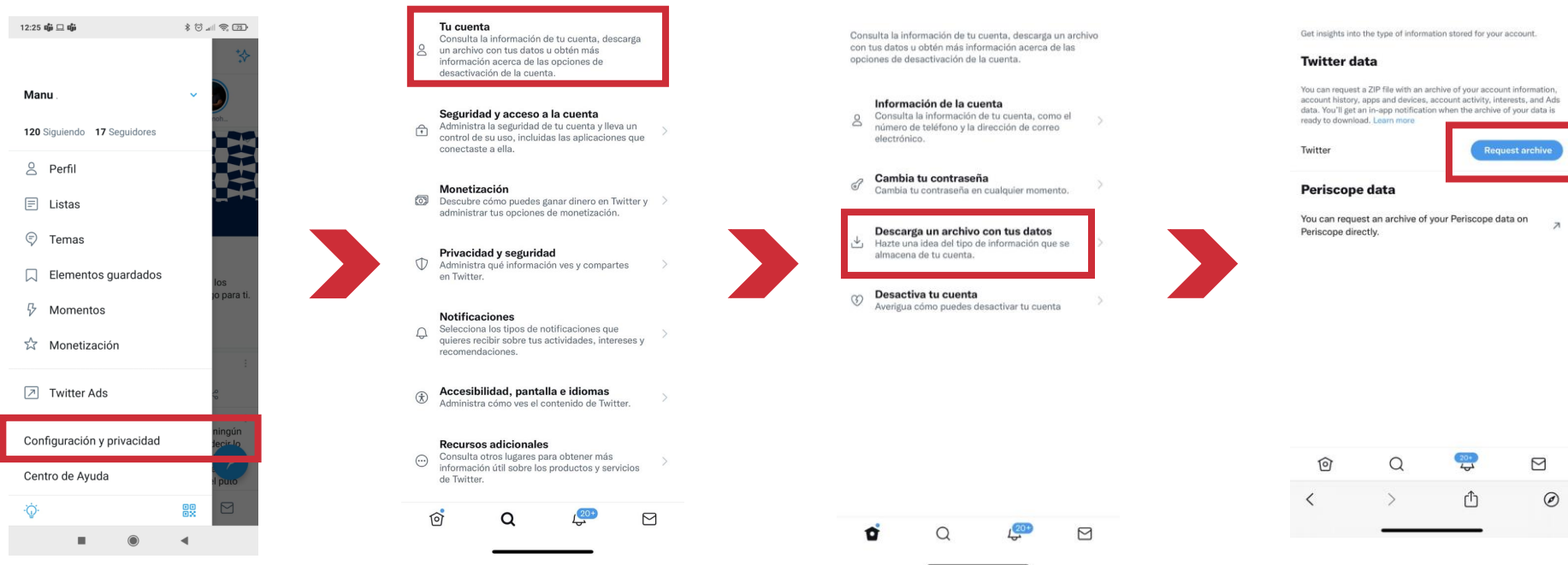
1. Accederemos a las opciones de perfil del usuario en **‘Configuración’ > ‘Seguridad’ > ‘Descarga de datos’**.
2. Luego nos pedirán confirmar nuestra contraseña y, en un **plazo de 48 horas**, nos enviarán la copia de seguridad.
3. Finalmente, recibiremos un correo electrónico con el **enlace para descargar** todos los datos asociados a nuestra cuenta.



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. DESCARGAR NUESTRA VIDA DE LAS REDES SOCIALES. TWITTER

Twitter nos permite descargar nuestra información en un archivo mediante los siguientes pasos:

Iremos a **‘Configuración y privacidad’ > ‘Tu cuenta’ > ‘Descargar un archivo con tus datos’ y, ‘Request archive’.**



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. PRACTICAR *EGOSURFING*

Internet es el mayor banco de información del mundo, pudiendo encontrar datos de cualquier cosa, incluido sobre nosotros mismos. Para saber qué información hay sobre nosotros en Internet existe una práctica conocida como *egosurfing*:

1. Podemos utilizar nuestro nombre, DNI, apellidos, dirección, teléfono, etc.
2. Es una practica que debemos realizar **periódicamente**.
3. Podemos hacerlo en **redes sociales u otras plataformas**.



2. BUENAS PRÁCTICAS AL UTILIZAR LAS REDES SOCIALES. PRACTICAR *EGOSURFING*

Para hacerlo, tan solo deberemos acceder a la red social que prefiramos e **introducir la siguiente información:**

1. Nombre y apellidos.
2. Nombre de usuario.
3. Correo electrónico.

En el caso de encontrar algo grave **podremos denunciarlo a la red social.**



ACTIVIDAD 2



Ahora que ya sabemos en qué consiste el *egosurfing*, deberíamos ser capaces de llevarla a la práctica.

Haz una búsqueda en Internet y en tus redes sociales sobre ti y apunta todo aquello que consideres importante, que contenga información personal o que no sabías que existía.

3. FRAUDES COMUNES EN REDES SOCIALES

El auge de las redes sociales y la inmensa cantidad de usuarios que las utilizamos las ha convertido en uno de los objetivos principales de los ciberdelincuentes. Los fraudes más comunes son:

1. Robo de cuentas.
2. Suplantación de identidad.
3. Contactos fraudulentos.
4. Anuncios y publicaciones a sitios web maliciosos.
5. Noticias falsas, bulos y cadenas de mensajes.
6. Concursos y promociones fraudulentas.
7. Sextorsión.



3. FRAUDES COMUNES EN REDES SOCIALES. ROBO DE CUENTAS

El robo de cuentas mediante ataques de ingeniería social y cuentas desprotegidas:

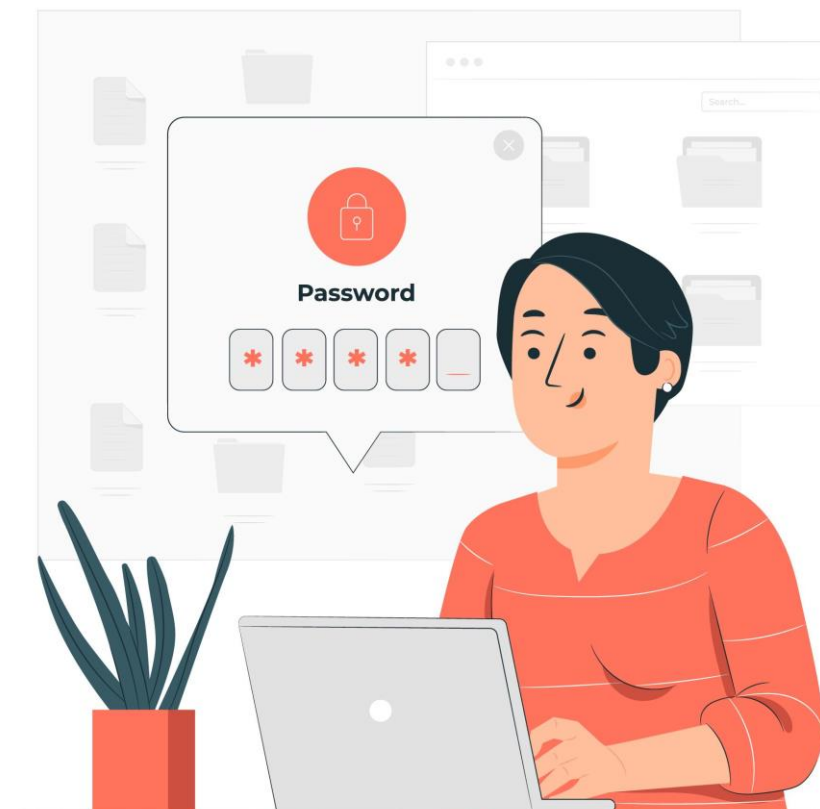
- Consiste en el uso de **técnicas de ingeniería social** para obtener nuestras credenciales por medio de engaños.
- O en el **ataque directo a nuestras contraseñas**.



3. FRAUDES COMUNES EN REDES SOCIALES. ROBO DE CUENTAS

¿Cómo nos protegemos?

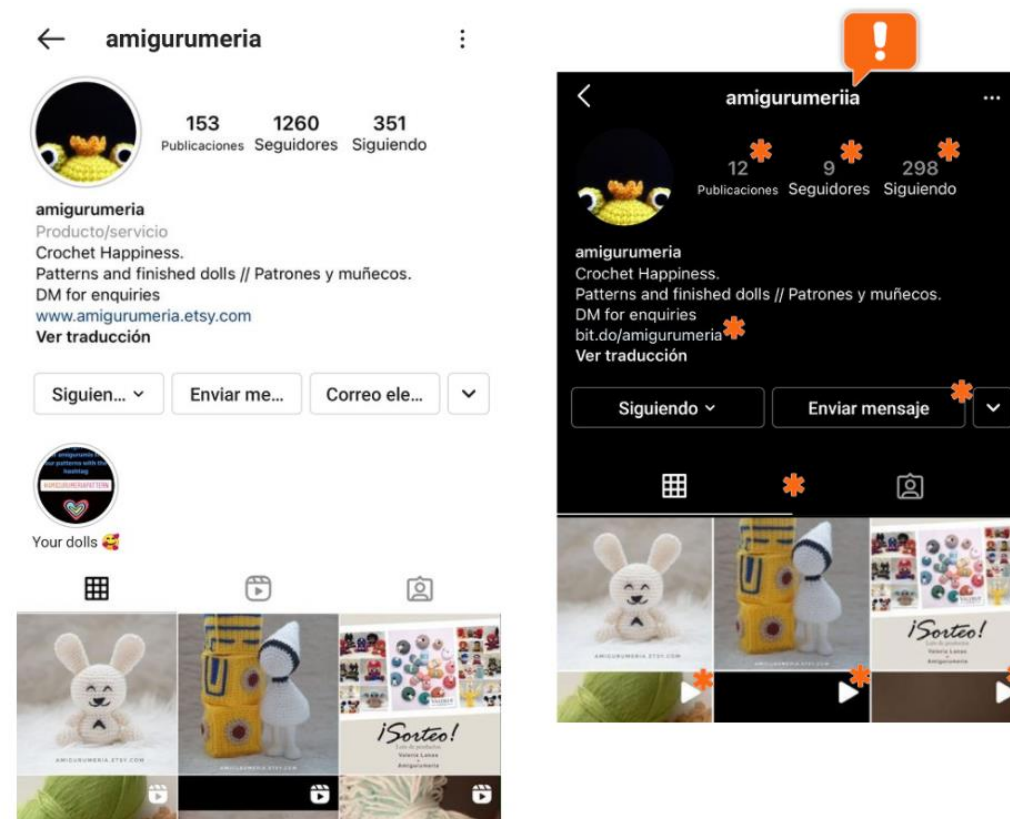
- Utilizar contraseñas robustas.
- No compartir las contraseñas.
- Activar la verificación en dos pasos.
- Evitar conectarnos en dispositivos públicos o diferentes de los habituales.
- Aplicar el sentido común.



3. FRAUDES COMUNES EN REDES SOCIALES. SUPLANTACIÓN DE IDENTIDAD (PERFILES FALSOS)

La **suplantación en redes sociales** es otro tipo de fraude muy común que consiste en la creación de perfiles falsos sirviéndose de la información publicada.

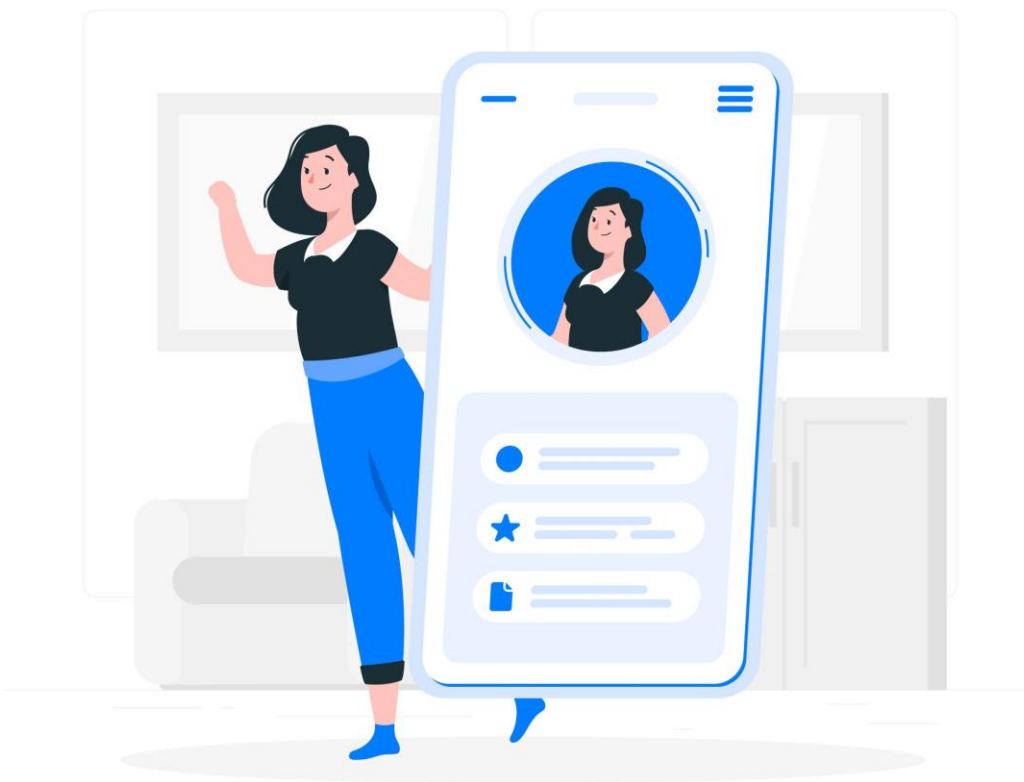
- Suplantan cuentas o marcas conocidas, así como personajes famosos o *'influencers'*. Aunque también pueden suplantar a usuarios comunes para engañar a sus contactos.
- Su ***modus operandi***:
 1. Obtienen toda la información pública, como fotos, vídeos o descripción.
 2. La utilizan para crear una cuenta casi idéntica.
 3. Aprovechará para enviar mensajes y enlaces a sus contactos.



3. FRAUDES COMUNES EN REDES SOCIALES. SUPLANTACIÓN DE IDENTIDAD (PERFILES FALSOS)

¿Cómo nos protegemos?

- Revisar la fecha de creación, seguidores y publicaciones de la cuenta.
- Comprobar la verificación de la cuenta.
- Desconfiar de peticiones de amistad de desconocidos.
- Comprobar el perfil en otras redes sociales.
- Configurar nuestras cuentas en modo privado.
- Practicar *egosurfing*.



3. FRAUDES COMUNES EN REDES SOCIALES. CONTACTOS FRAUDULENTOS

Las redes sociales son plataformas para compartir nuestra vida con nuestros contactos, sin embargo, **existe una creencia falsa de que cuanto más contactos tengamos, mejor**. Esta práctica **puede ocasionarnos más problemas que beneficios**:

- Pueden enviarnos enlaces maliciosos o archivos infectados.
- Noticias falsas, bulos y cadenas de mensajes.
- Realizar publicaciones ofensivas o controvertidas en nuestro muro.
- Problemas de privacidad si compartimos información personal con desconocidos.



3. FRAUDES COMUNES EN REDES SOCIALES. CONTACTOS FRAUDULENTOS

¿Cómo nos protegemos?

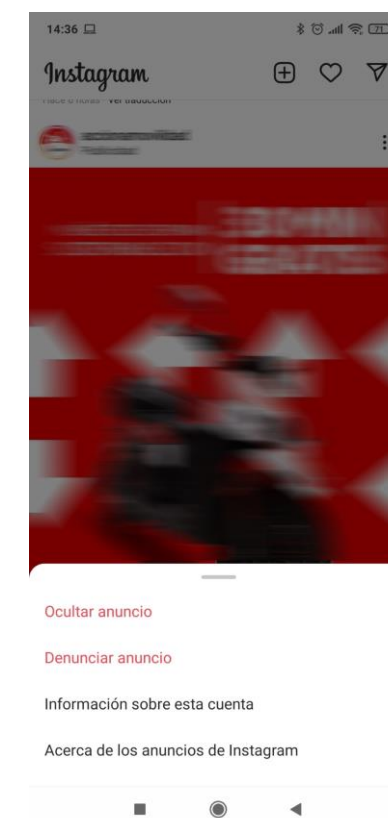
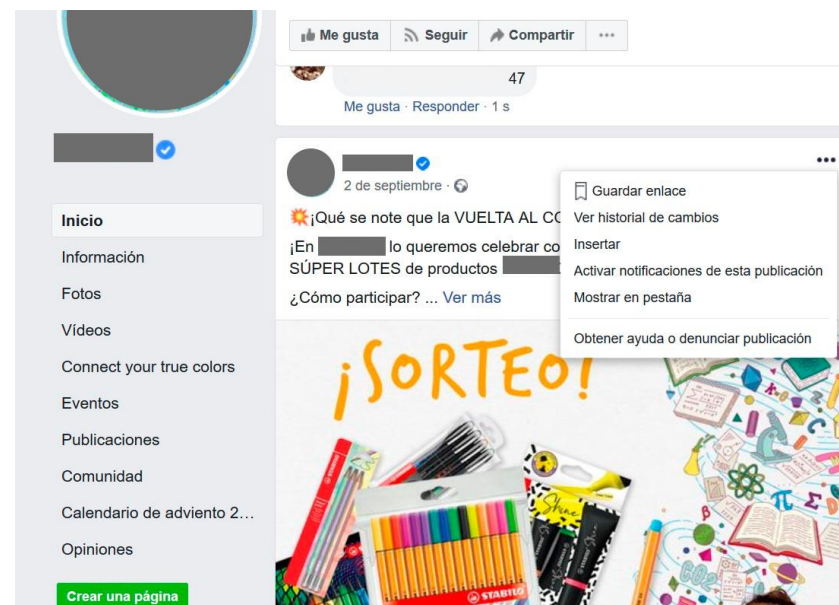
- Limpiar nuestra red de contactos desconocidos o sospechosos.
- Configurar nuestro perfil para evitar mensajes de desconocidos.
- Comprobar los perfiles de estos usuarios para asegurarnos.
- Bloquear y eliminar usuarios si es necesario.



3. FRAUDES COMUNES EN REDES SOCIALES. ANUNCIOS Y PUBLICACIONES MALICIOSAS

Las redes sociales se financian por medio de anuncios publicitarios para evitar que los usuarios tengamos que pagar por registrarnos. Sin embargo, algunos ciberdelincuentes aprovechan para ‘colar’ anuncios y publicaciones maliciosas:

- **Enlaces a webs poco fiables o maliciosas** que nos instalen algún *malware*, por ejemplo.
- **Enlaces a webs que suplantan la identidad de otras legítimas** para hacerse con nuestros datos.



3. FRAUDES COMUNES EN REDES SOCIALES. ANUNCIOS Y PUBLICACIONES MALICIOSAS

¿Cómo nos protegemos?

- Denunciar publicaciones de anuncios sospechosos o maliciosos.
- Añadir mecanismos para bloquear anuncios en redes sociales e Internet.
- Analizar el contenido para detectar si es o no fraudulento.
- Analizar la URL para detectar si es segura (certificado y HTTPS).



3. FRAUDES COMUNES EN REDES SOCIALES. BULOS Y FAKE NEWS

Las **noticias falsas** han encontrado en las redes sociales un medio por el que viralizarse y extenderse mucho más rápidos que las noticias reales.

- Causan **desinformación y desconfianza** entre la población.
- Son una **amenaza para la identidad digital** al desprestigiar o atacar a personas o empresas.

Bill Gates reconoce que miles de personas morirán con la vacuna del coronavirus

El magnate de la tecnología en una entrevista reveló su teoría sobre la vacuna y sorprendió a todos.



Por Diario26

Martes 12 de mayo de 2020



Bill Gates, fundador de Bill & Melinda Gates Foundation.

En una entrevista reciente que Bill Gates brindó en el canal CNBC de los Estados Unidos,

MAS LEIDAS

Diario26

1. Fabián "Pepin" Rodríguez Simón pidió asilo político en Uruguay
2. El Gobierno estudia nuevas restricciones por coronavirus y "un cierre fuerte" desde este fin de semana
3. Dolor en el deporte argentino: murió por coronavirus el nadador paralímpico Jorge Corvalán
4. Nuevo Orden Mundial: el plan siniestro para "matar sin que se note"
5. En medio de la escalada de precios, el Gobierno decidió suspender la exportación de carne por 30 días

3. FRAUDES COMUNES EN REDES SOCIALES. BULOS Y FAKE NEWS

¿Cómo nos protegemos?

- Buscar las fuentes y contrastar la noticia en Internet.
- Revisar la URL para comprobar si es una web fiable.
- Analizar el titular para identificar su objetivo.
- Comprobar el formato de la noticia.



3. FRAUDES COMUNES EN REDES SOCIALES. CONCURSOS FRAUDULENTOS



GOBIERNO
DE ESPAÑA
VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



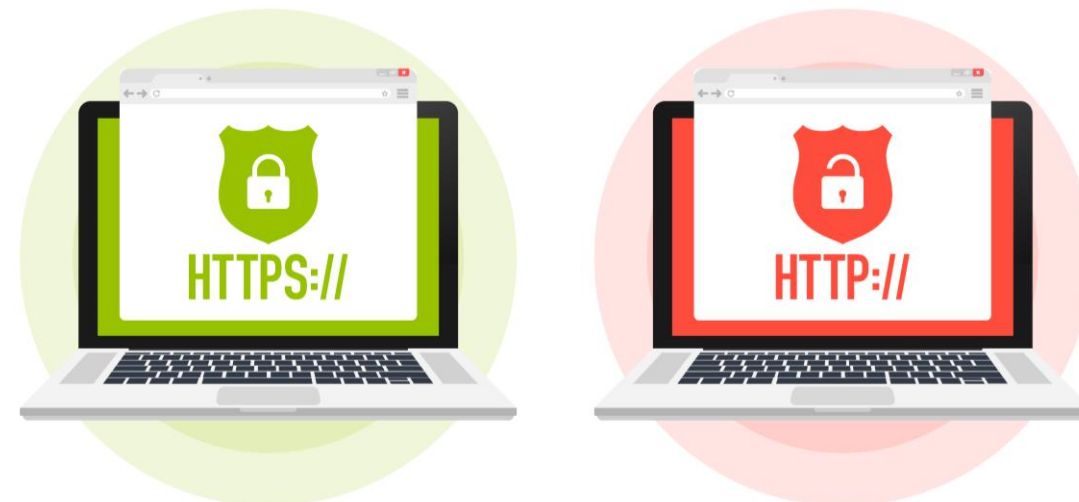
Hoy en día, los concursos, promociones y sorteos en redes sociales se han convertido en una actividad muy popular. Los ciberdelincuentes los aprovechan **para engañarnos y conseguir nuestros datos o distribuir *malware*.**



3. FRAUDES COMUNES EN REDES SOCIALES. CONCURSOS FRAUDULENTOS

¿Cómo nos protegemos?

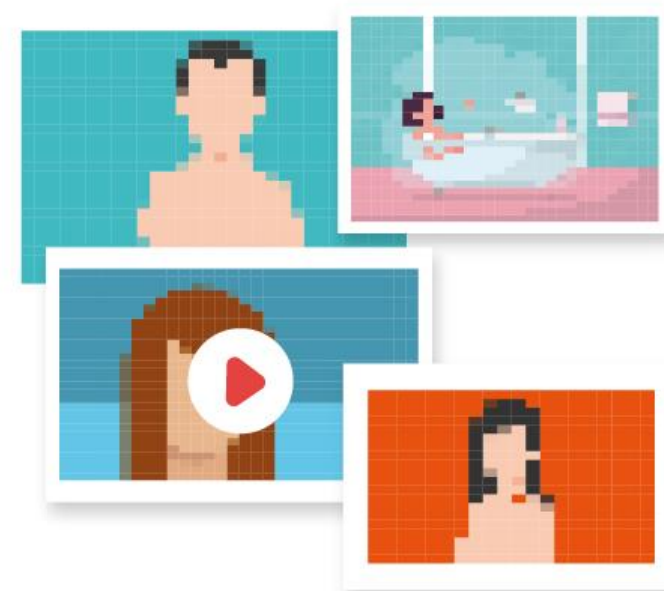
- Comprobar la marca y el concurso en otras redes.
- Revisar las bases legales del concurso.
- Comprobar la URL para ver si es segura (HTTPS y certificado).
- Analizar los comentarios de otros usuarios.
- Revisar el formato en busca de fallos.
- Contrastar las imágenes y comprobar que no sean robadas.



3. FRAUDES COMUNES EN REDES SOCIALES. **SEXTORSIÓN Y AMORES EN LÍNEA**

Uno de los objetivos de las redes sociales es que socialicemos y nos relacionemos con otros usuarios. En ocasiones, los ciberdelincuentes se hacen pasar por usuarios con los que empezamos a intimar (**sexting**) y esto puede desembocar en **sextorsión**.

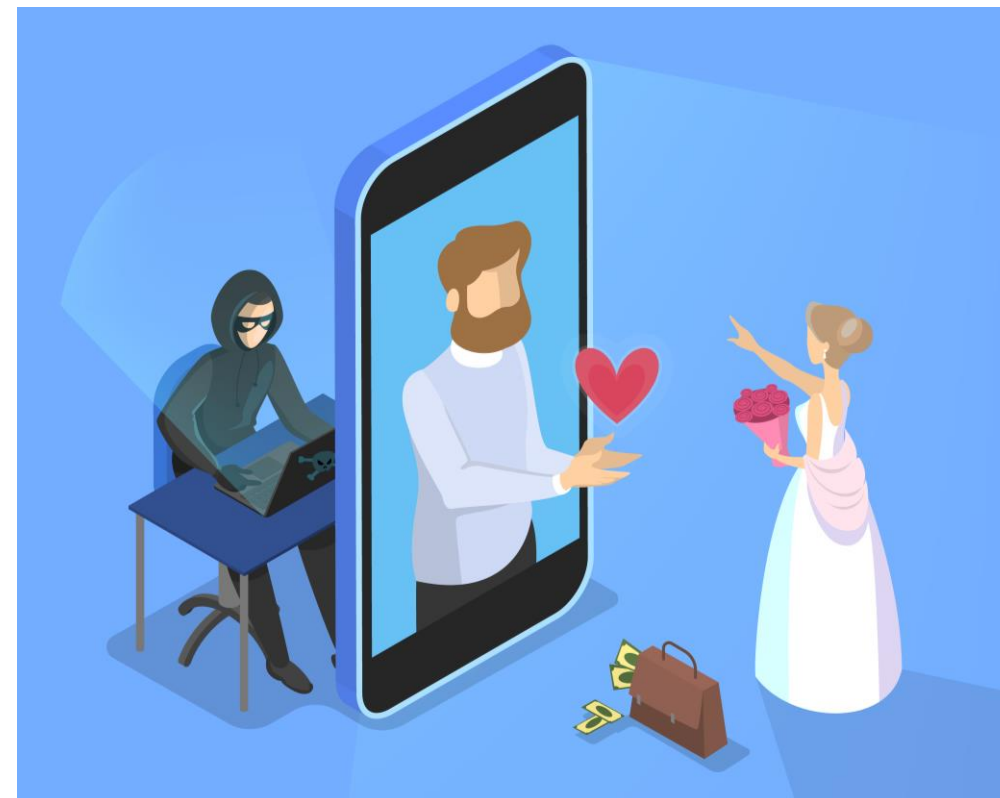
- **Sexting**: intercambio de contenidos de carácter sexual e íntimo (fotografías o vídeos) entre dos usuarios a través de Internet de forma consensuada.
- **Sextorsión**: fraude que consiste en enviar correos o mensajes a los usuarios solicitando dinero o más contenido sexual a cambio de no divulgar fotografías o vídeos íntimos sobre ellos.



3. FRAUDES COMUNES EN REDES SOCIALES. *SEXTORSIÓN Y AMORES EN LÍNEA*

¿Cómo nos protegemos?

- No revelar y evitar compartir información personal con desconocidos.
- Investigar a nuestros contactos nos ayudará a descartar potenciales ciberdelincuentes.
- Nunca enviar dinero, ya que el pago no garantiza nada.
- Evitar descargar archivos o entrar a enlaces sospechosos que puedan contener *malware*.



CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



1. Lo que publicamos en Internet, fotos, vídeos, opiniones, etc., así como toda la información que existe en Internet sobre nosotros se conoce como:

- A. Identidad digital.
- B. Identidad social.
- C. Identidad online.

CUESTIONARIO DE EVALUACIÓN



VICEPRESIDENCIA
PRIMERA DEL GOBIERNO
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Responde a la siguiente pregunta:



2. ¿Cuál de las siguientes informaciones no debemos compartir en redes sociales bajo ningún concepto?

- A. Fotografía de un viaje.
- B. Dirección personal.
- C. Opinión sobre una película.



TU AYUDA EN
CIBERSEGURIDAD
incibe



Oficina
de Seguridad
del Internauta

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



3. Realizar una búsqueda en la Red de nuestro nombre, teléfono o correo electrónico para ver qué se dice de nosotros, se conoce como:

- A. *Egosurfing.*
- B. Autobúsqueda.
- C. *Egosearching.*

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



4. Una de nuestras redes sociales nos ha enviado un correo avisándonos de una actividad sospechosa en nuestra cuenta. ¿Qué deberíamos hacer?

- A. Configurar la privacidad de nuestra cuenta.
- B. Cambiar las contraseñas.
- C. Eliminar contactos.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



5. ¿Cómo podemos identificar perfiles falsos en una red social?

- A. Revisando su información y contactos.
- B. Comprobando la fecha de creación y sus publicaciones.
- C. Ambas opciones.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



6. Mientras navegamos por nuestra red social favorita, encontramos un anuncio sobre un producto que nos llama la atención. ¿Qué debemos hacer?

- A. Analizar los comentarios.
- B. Comprobar la URL.
- C. Ambas opciones.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



7. Las noticias falsas son muy comunes hoy en día, ¿qué pasos debemos seguir para identificarlas?

- A. Buscar la fuente, revisar la URL, ver el número de visitas.
- B. Buscar la fuente, revisar la URL, comprobar el titular y el formato.
- C. Analizar el contenido, los 'likes' y el número de visitas.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



8. Imaginemos que un usuario con el que llevamos tiempo hablando por Internet, comienza a pedirnos imágenes de tipo íntimo o sexual. ¿A qué tipo de fraude nos estamos exponiendo?

- A. *Egosurfing.*
- B. *Phishing.*
- C. *Sextorsión.*

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



9. Algunas de las funciones que podemos activar desde la configuración de privacidad de nuestra cuenta en redes sociales, es:

- A. Modificar la contraseña de nuestra cuenta.
- B. Limitar la visibilidad de nuestro perfil.
- C. Activar la verificación en dos pasos.

CUESTIONARIO DE EVALUACIÓN

Responde a la siguiente pregunta:



10. Una medida de seguridad muy recomendada es activar la función para recibir un código temporal en nuestro dispositivo móvil cada vez que queramos iniciar sesión. ¿Cómo se denomina esta función?

- A. Doble inicio de sesión.
- B. Bloqueo en dos pasos.
- C. Autenticación en dos pasos.



INSTITUTO NACIONAL DE CIBERSEGURIDAD

Gracias por vuestra atención



GOBIERNO
DE ESPAÑA

VICEPRESIDENCIA
PRIMERA DEL GOBIERNO

MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL

SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN E
INTELIGENCIA ARTIFICIAL



TU AYUDA EN
CIBERSEGURIDAD




Oficina
de Seguridad
del Internauta

LICENCIA DE CONTENIDOS

La presente publicación pertenece a Instituto Nacional de Ciberseguridad (INCIBE) y está bajo licencia Reconocimiento-No Comercial-CompartirIgual 4.0 Internacional de Creative Commons. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- ❖ Reconocimiento. El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa a INCIBE y su sitio web: <https://www.incibe.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- ❖ Uso No Comercial. El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- ❖ Compartir Igual. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia: https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es_ES



**Reconocimiento-NoComercial-CompartirIgual 4.0
Internacional (CC BY-NC-SA 4.0)**