

9 GUÍA de CIBERSEGURIDAD



DESDE LOS 12 HASTA LOS 18 AÑOS



GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR



DIRECCIÓN GENERAL
DE LA GUARDIA CIVIL



Realizado por
UCCIBER
(Unidad de
Coordinación
de Ciberseguridad)
© Dirección General de
la Guardia Civil
<http://www.guardiacivil.es>

Catálogo de Publicaciones de la
Administración General del Estado
<https://cpage.mpr.gob.es>

Edita : Secretaría General Técnica del Ministerio
del Interior

Reservados todos los derechos
Prohibida la reproducción total o parcial sin
la debida autorización.
NIPO (ed. papel): 126-23-036-5
NIPO (ed. en línea): 126-23-037-0
Depósito Legal: M-16580-2023





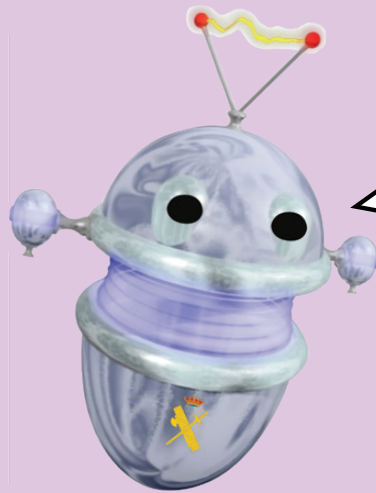
Los datos revelan que la mayoría de los adolescentes (más del 90%) tiene a su disposición un móvil con conexión a Internet y conexión wifi en casa, lo que les permite estar casi permanentemente conectados a Internet.

La cibercriminalidad es un desafío en constante evolución en todo el mundo, y España no es una excepción. Con cada avance de la informática y de las telecomunicaciones, los ciberdelincuentes encuentran nuevas formas de cometer delitos online.

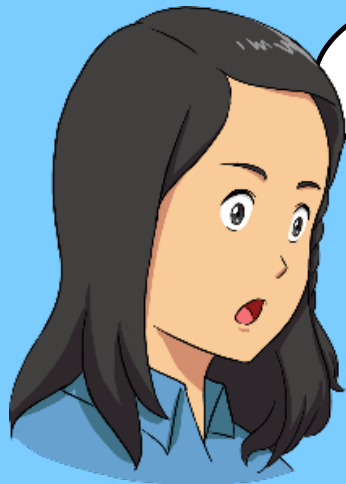
La Guardia Civil, para hacer frente a esta situación y proteger a los usuarios de Internet, dedica numerosos esfuerzos para prevenir y combatir el cibercrimen.

La Guardia Civil ha creado los Equipos @, que se encargan de asesorar, prevenir y luchar contra la cibercriminalidad, especialmente contra las estafas en la red. Se encuentran en todas las provincias, y una de sus funciones es proporcionar atención presencial y a distancia a los ciudadanos.

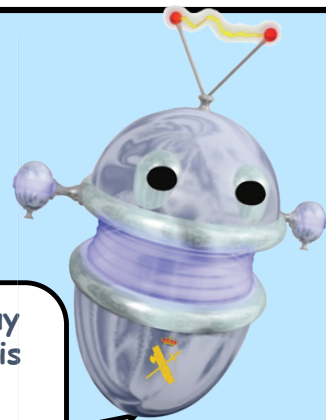




¿Conocéis los peligros a los que os exponéis en Internet?



¿Peligros?
¿Nosotros?



Internet es muy **útil**, pero debéis conocer los peligros que esconde para saber protegeros



Queremos conocer los peligros que hay en Internet.
¿Nos ayudas?



ESTOS SON LOS PRINCIPALES PELIGROS QUE OS PODÉIS ENCONTRAR EN INTERNET

CONTENIDOS INAPROPIADOS

Son aquellos que no están acordes con tu edad o que muestran información nociva (pornografía, violencia, juego, maltrato animal, apología de la anorexia y la bulimia,...).

GROOMING

Engaño y acoso de un mayor a un menor, a través de redes sociales y chats de juego, con intenciones sexuales.

CYBERBULLING

Mensajes ridiculizando e insultando a compañeros poco populares o menos divertidos. Piensa en cómo te sentirías si se refieren a ti, y si los reenvías

puedes ser autor de un delito que se paga con la cárcel.

SEXTING

Obtener fotos de contenido sexual o eróticas de la víctima para extorsionarla.

PHISHING

Emails que suplantan la identidad de terceros y que, mediante engaño, te inducen a facilitar datos personales o a instalar programas no deseados. Si es a través de mensajes sms, se conoce como smishing.

SUSCRIPCIONES O COMPRAS NO DESEADAS

A través de mensajes engañosos con eslóganes de "gratis"

o "regalo de bienvenida", pueden engañarte para que te suscribas a servicios no deseados vinculados a tu teléfono móvil. Tiene especial gravedad el acceso a salones de juego online, con promesas de ganancias seguras.

MENTIRAS EN LA RED

También conocidas como fake news. Es información falsa que busca condicionar tu conducta y opinión sobre conocidos.

MALWARE

Programas maliciosos que buscan robar información de tus equipos informáticos o smartphones, o espiar tus conversaciones.

¿Pero cómo puedo protegerme en las redes sociales?



NO AGREGUES A CUALQUIER PERSONA

En nuestras redes sociales solemos compartir mucha información personal (nuestras fotos, las de familiares y amigos, nuestras preferencias y gustos, sitios a los que vamos de vacaciones, lugares que frecuentamos, etc.). Cuando agregas a una persona que no conoces, le estás dando acceso a toda esa información y no sabes qué va a hacer con ella.



PROTEGE TUS DATOS PERSONALES

Existen muchas opciones de seguridad en cada una de las redes sociales para que puedas gestionar adecuadamente qué pueden y qué **NO** pueden ver tus contactos.

Incluso si tienes una cuenta abierta, no tienes por qué compartir todas tus publicaciones, sino que puedes seleccionar quienes las pueden ver.



CONTROLA QUIÉN VE TU INFORMACIÓN ¿CÓMO PUEDES CONFIGURAR TU IPHONE?

En **Configuración**, haz clic en **Cuenta** y luego en **Privacidad**. Esto permite que vean tu **Foto de perfil, Info, Estado y Hora de última vez sólo quien tú quieras**



WhatsApp

En **Configuración y privacidad**, haz clic en **Privacidad de la Cuenta** y selecciona **Cuenta Privada**



Instagram

En **Ajustes y Privacidad**, haz clic en **Privacidad** y luego en **Privacidad**, selecciona **Cuenta Privada**



Tik Tok

En **Configuración**, ve desactivando las localizaciones por número de teléfono o correo electrónico, y en **Controles de Privacidad** selecciona uno a uno para securizarlo



SnapChat

CONTROLA QUIÉN VE TU INFORMACIÓN ¿CÓMO PUEDES CONFIGURAR TU ANDROID?



En **Ajustes**, haz clic en **Privacidad**. Esto permite que vean tu **Foto de perfil**, **Info**, **Estado** y **Hora de última vez** sólo quien tú quieras



WhatsApp

Desde la pantalla de **Perfil**, toca y selecciona **Ajustes** y **Privacidad**, haz clic en **Privacidad** y selecciona **Cuenta Privada**



Tik Tok

Desde la pantalla de usuario, toca y selecciona **Configuración** y **privacidad**, haz clic en **Privacidad de la Cuenta** y selecciona **Cuenta Privada**



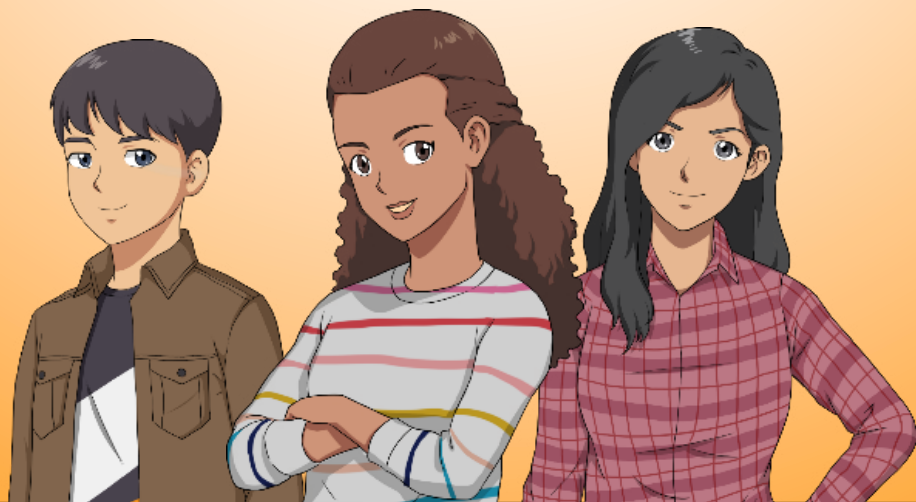
Instagram

En **Configuración**, ve desactivando las localizaciones por número de teléfono o correo electrónico, y en **Controles de Privacidad** selecciona uno a uno para securizarlo



SnapChat

Creo que estoy más
tranquila ahora
sabiendo que puedo
protegerme en las
redes sociales



Claro que sí. Pues ahora no
dejes de compartir lo que has
aprendido con tus amigos, para
que todos estemos protegidos



LOS CONSEJOS DEL CIBER GUARDIA CIVIL

Usa
Contraseña segura
y, si es posible, doble
factor de autenticación
(2FA).

**¡Y contraseñas
distintas para
distintos servicios!**

**No compartas
imágenes íntimas
ni información
personal por
Internet**

**Configura
tus perfiles
de usuario
con la máxima
privacidad**

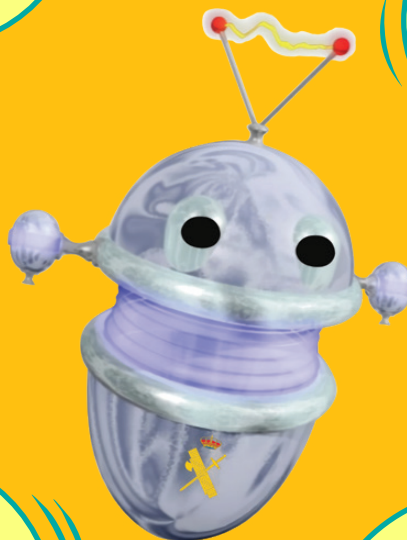
**No abras
mensajes de
gente que no
conoces y
bajo ningún concepto
abras ni descargues
los adjuntos
del mensaje.
Pueden contener
malware**

**Huye de las
apuestas y el
juego online.
La probabilidad
de ganar dinero
es ínfima**

**Huye de lo
gratuito y de los
regalos de bienvenida
en Internet. Y
nunca des tus
datos personales**

**Todo lo que
escribas o cuelgues
en Internet, queda
para siempre.
Asegúrate.
No te
arrepentirás**

**No te creas
todo lo que se dice
en Internet.
Hay personas que se
inventan o mienten
para que tú
cambies de
opinión**



RECUERDA:

SÉ AMABLE Y RESPETUOSO EN LAS REDES SOCIALES

Detrás de cada perfil hay una persona real. Trata a los demás como te gustaría que te tratasen a ti, incluso cuando no estés de acuerdo con ellos. Evita participar en discusiones negativas o inútiles.

Y si alguien o algo te molesta o te hace sentir incómodo en Internet, háblalo

con tus padres, tutores, profesores, o acude al Equipo @ de tu provincia. No dejes que se te "haga bola". A veces, lo que empieza como un juego, acaba como un delito.

Y por último, disfruta de Internet, pero también disfruta de hacer deporte, salir con tus amigos o de cualquier afición. No caigas en la adicción. Hay más vida que Internet.

062
GUARDIA CIVIL



Recuerda
este número
de teléfono





Dirección General de la Guardia Civil
Unidad de Coordinación de Ciberseguridad
C/ Guzmán El Bueno 110 – 28003 Madrid
www.guardiacivil.es – Telf.: 900.101.062



EDITA: SECRETARÍA GENERAL TÉCNICA DEL MINISTERIO DEL INTERIOR
CATÁLOGO DE PUBLICACIONES DE LA ADMINISTRACIÓN GENERAL DEL ESTADO
<https://cpage.mpr.gob.es>
REALIZADO POR LA UCCIBER (UNIDAD DE COORDINACIÓN DE CIBERSEGURIDAD)



PETEC ASOCIACIÓN PROFESIONAL
DE PERITOS DE NUEVAS TECNOLOGÍAS

