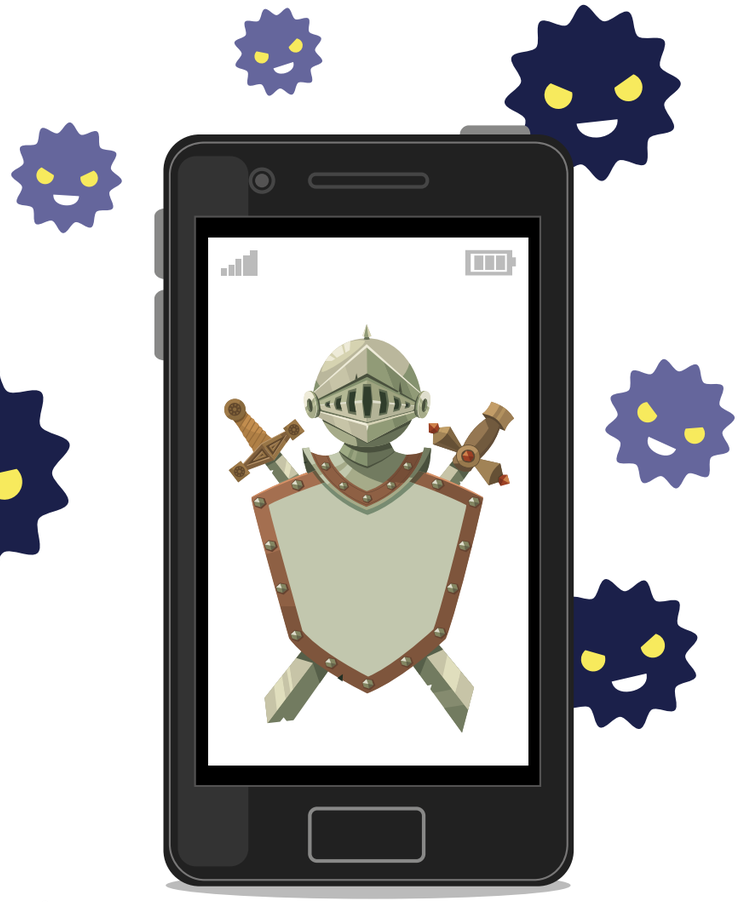
Teléfono móvil en alerta

El número de ataques a *smartphones* ha aumentado de forma notable en los últimos años, pero se pueden minimizar los riesgos



Los delincuentes no descansan. Siempre buscan formas de delinquir adaptadas a los nuevos tiempos. En la actualidad, son conscientes de que el número de teléfonos móviles que se conectan a Internet en España es superior al de ordenadores. Por lo que han puesto su mirada en los *smartphones*, cuya pérdida o sustracción pone en peligro la privacidad y seguridad de los usuarios, igual que lo hace un ataque informático.

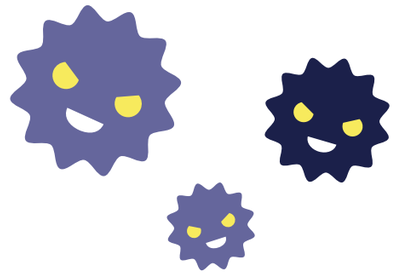
Por este motivo, es importante seguir algunas recomendaciones y consejos para hacer más seguro el teléfono móvil. Aunque no existe el 100% de protección, se pueden minimizar riesgos:

1. Instalar aplicaciones desde las tiendas oficiales.

Los sistemas operativos Android, iOS y Windows Phone cuentan con sus propias tiendas de aplicaciones. En general, estas tiendas disponen de diferentes mecanismos para controlar aquellas *apps* que incluyen códigos maliciosos o que ponen en peligro la privacidad de los usuarios. Algunas veces, se han distribuido aplicaciones maliciosas en estas tiendas, pero no es frecuente y siempre se ha alertado a los usuarios.

2. Obviar los mensajes de alerta en páginas web.

Los usuarios de Android deben tener en cuenta que, por las características del sistema operativo, la mayoría de los ataques se dirigen a esta plataforma mediante engaños y mensajes. Por este motivo, es importante no hacer caso a anuncios en forma de *pop-ups* o *banners* de diferentes páginas web donde, por ejemplo, se alerta al usuario de que su teléfono móvil está infectado y que tiene que instalar un archivo con extension .apk (el formato de las aplicaciones de Android). Al hacerlo, el usuario instala sin saberlo una aplicación maliciosa que toma el control de su terminal.



3. Cuidado con el *jailbreak* y la instalación de ROMs de fuentes desconocidas.

Liberar el terminal, un proceso conocido como *jailbreak,* solo está recomendado para usuarios que saben lo que están haciendo, ya que su uso indiscriminado y la instalación de ROMS o versiones especiales del sistema operativo de fuentes desconocidas, puede poner en peligro la seguridad del usuario que desconoce las intenciones de los desarrolladores.

4. Bloqueo del teléfono con el código PIN

Permite que, en el caso de que alguien se haga con el teléfono, no pueda acceder a los datos del usuario. Es una medida de seguridad esencial en el teléfono móvil. Por lo general, este número es de cuatro dígitos, pero se puede hacer más largo en iPhone. Solo hay que ir a "Ajustes-General-Bloqueo con código" y deshabilitar la opción "Código simple".

5. Cifrar el contenido del teléfono.

De esta forma, se evita el acceso no autorizado al terminal en el caso de conectar el teléfono a una *wifi* pública o mediante conexión a un ordenador, entre otras situaciones. Las últimas versiones tanto de iOS como de Android cuentan con mecanismos para cifrar los datos de los usuarios en una opción activada por defecto. En el caso de utilizar tarjetas SD o versiones anteriores de Android, se pueden cifrar desde el apartado de seguridad de los ajustes generales.

6. Verificación de los archivos alojados en la nube.

La sincronización de archivos en la nube otorga muchas ventajas a los usuarios, ya que permite acceder a los datos desde cualquier dispositivo y lugar. Sin embargo, para dotar de una mayor protección a estos datos personales, es importante mejorar la seguridad en el acceso a los datos. En el caso de DropBox o iCloud, es recomendable activar en las opciones generales la verificación en dos pasos. De esta forma, aunque alguien se haga con la contraseña de acceso del usuario, es necesario incluir un código de seguridad enviado mediante SMS al terminal.

7. Activar "localizar el terminal".

Tanto iOS como Android cuentan con una opción para localizar el teléfono móvil en caso de pérdida o sustracción. Esta herramienta permite localizar fácilmente un terminal extraviado si este está conectado a Internet y tiene activado el GPS. De esta forma, se muestra sobre un mapa el lugar aproximado donde se encuentra. Otras opciones muy interesantes sirven para activar una alarma en el teléfono o bien realizar un borrado remoto del dispositivo. En iOS, esta opción se activa en "Ajustes- iCloud-Buscar mi iPhone". Por su parte, en Android, hay que acceder a "Ajustes-Seguridad-Activar el Administrador de Dispositivos". En el caso de no tenerla instalada, la herramienta de localización se puede descargar desde Google Play.

8. Mantener actualizado el software.

Es una de las mejores formas de minimizar los riesgos de seguridad. La mayoría del *malware* distribuido se aprovecha de vulnerabilidades no resueltas o de algunas disponibles en versiones antiguas.

9. Cuidado con las redes *wifi* libres o de terceros en espacios públicos.

Conectarse a una *wifi* desconocida pone en peligro la seguridad y privacidad del dispositivo, pues todo el tráfico que no vaya cifrado por las aplicaciones puede ser capturado por un tercero, lo que incluye contraseñas, credenciales a banca online o mensajes personales. Es aconsejable utilizar un servicio de VPN, ya que cifra todo el tráfico del usuario cuando accede a Internet.

10. Realizar copias de seguridad.

Las copias de seguridad de los datos del teléfono móvil permiten recuperar su contenido ante cualquier problema. En iOS, estas copias se pueden realizar automáticamente mediante iCloud o iTunes. En Android, los usuarios disponen de diferentes opciones para hacer copias de seguridad, ya que no todos los móviles con el sistema operativo de Google tienen por defecto esta opción. //