3 Prevención de virus y fraudes

- 3.1 Definición y conceptos
- 3.2 Datos y ejemplos
- 3.3 Pautas y recomendaciones
- 3.4 Estrategias de prevención

Copyright 2026

3.1 Definición y conceptos

DEFINICIÓN Y CONCEPTOS

El término “virus” se utiliza comúnmente para referirse a las aplicaciones informáticas que buscan alterar el funcionamiento de los dispositivos (PC, tabletas, smartphones, etc.) y en muchos casos, robar información del usuario. Existen numerosos tipos de programas maliciosos que se han vuelto más sofisticados y más peligrosos, y más difíciles de detectar.

Al principio los virus solían centrar su actividad en causar molestias al usuario, borrando información, impidiendo el uso de determinados programas o ralentizar el arranque del ordenador.

Por desgracia, **la mayoría de los virus actuales tienen como objetivo el obtener información de los usuarios infectados**, tales como datos bancarios fotos, contraseñas o uso de la webcam.

Hoy en día existen muchos **programas maliciosos** que permiten tomar el control absoluto del ordenador y realizar cualquier tipo de acción sin nuestro conocimiento, como por ejemplo:

- Suplantar nuestra identidad y enviar correos electrónicos en nuestro nombre.
- Utilizar nuestro ordenador para realizar ataques a otros ordenadores.
- Realizar estafas en las que figurará nuestro ordenador (y nuestra IP) como origen del delito.
- Enviar publicidad.
- Secuestrar y cifrar nuestros archivos, y exigir un pago para recuperarlos.

Los ciberdelincuentes utilizan diversas **técnicas para infectar los sistemas con virus**, como por ejemplo:

- La infección puede llevarse a cabo al instalar un archivo o un programa supuestamente legítimo pero que contiene código malicioso porque haya sido pirateado.
- La infección puede producirse simplemente conectándote a una web infectada, aprovechando una vulnerabilidad (fallo de seguridad) en el sistema operativo, en el navegador, en plugins y aplicaciones que los usuarios utilizan habitualmente
- Otra forma de infección se produce cuando se pulsa sobre un enlace malicioso recibido a través de alguna aplicación de mensajería (por ejemplo, WhatsApp, Twitter, o Facebook). En el momento de pulsar el enlace se redirige al usuario a una web en la que se produce

Copyright 2026

la infección. El gancho para pulsar sobre el enlace suele consistir en una invitación para ver una noticia llamativa.
- Los dispositivos externos como pen drives también pueden incluir virus que infecten los ordenadores.
- Algunas estrategias de engaño pueden infectar tu equipo, por ejemplo cuando recibes un mensaje indicándote que proporciones tus datos de clave de usuario y contraseña para activar tu cuenta, alegando un falso mantenimiento del servicio.

En la actualidad **existen virus para todas las plataformas y dispositivos**, por lo que cualquier ordenador conectado a Internet es susceptible de ser infectado por un virus, independientemente de la plataforma (Windows, Apple, Linux) o el dispositivo (ordenador, tabletas, teléfono móvil).

A estos riesgos, hay que añadir que los menores poseen ciertas características tales como inocencia, curiosidad, inexperiencia o impaciencia, que los pueden hacer especialmente débiles al potenciar los riesgos de infección y fraude.

Tipos de fraude online

Los fraudes electrónicos pueden ser muy variados. En algunos casos, se estudian los hábitos de la víctima (especialmente a través de la redes sociales), y se busca ganar su confianza para eliminar protecciones (por ejemplo, se suele aconsejar desactivar el antivirus para que el ordenador vaya más rápido).

En otros casos, se recurre a incluir condiciones en unos términos ambiguos antes de instalar un juego o programa, confiando en que el usuario aceptará las condiciones de instalación sin leerlas, especialmente, si se trata de un menor.

Algunos **tipos de fraude online** que te puedes encontrar en tu actividad diaria en la red son:

- **Rogue software o fakeav**: Se le denomina Rogue Software (o también Rogue Rogueware, FakeAVs, Badware, Scareware) a los “Falsos programas de seguridad” que no son realmente lo que dicen ser, sino que todo lo contrario. Bajo la promesa de solucionar falsas infecciones, cuando el usuario instala estos programas, su sistema es infectado. Estos falsos Antivirus y Antispyware están diseñados para mostrar un resultado predeterminado (siempre de infección) y no hacen ningún tipo de escaneo real en el sistema al igual que no eliminaran ninguna infección que podamos tener. La estafa consiste en invitarnos a descargar la versión completa del programa de protección solicitando para ello el pago, por medios “poco seguros”, de cierta cantidad de dinero
- **Phishing**: Es una actividad delictiva encaminada al robo de contraseñas personales y credenciales bancarias, es decir a la “pesca de contraseñas” que ya explicamos en el tema anterior.

Copyright 2026

- **Suscripción a servicios Premium o de pago**: Existen aplicaciones fraudulentas para dispositivos móviles que envían mensajes SMS Premium desde nuestro teléfono sin que seamos conscientes de ello hasta que recibimos la factura. A veces la información suele hallarse camuflada en el listado de condiciones que debemos aceptar antes de instalar una aplicación. Cuando pulsamos el botón y aceptamos la instalación, estamos dando nuestro consentimiento para que la aplicación envíe mensajes SMS Premium en nuestro nombre, cuyo coste será cargado en nuestra factura. Este tipo de fraudes se produce muy a menudo en la descarga de juegos, aprovechando la ingenuidad de nuestros menores.
- **Fraudes vinculados al mundo del videojuego.** Otro de los aspectos que aprovechan los ciberdelincuentes es el hecho de que muchos menores utilizan la misma clave de acceso y contraseña para distintos servicios lo que aumenta aún más el riesgo de robo de información personal cuando se es víctima de una estafa. Entre los más importantes tenemos la suscripción oculta y con coste y el robo de tatos. En el primer caso se produce al hacer clic en la publicidad de aplicaciones para móviles. En el segundo caso se produce en algunos juegos muy populares que te ofrecen algunos trucos o vidas infinitas ofreciendo a cambio sus datos de acceso a sus redes sociales.

Copyright 2026

3.2 Datos y ejemplos

ALGUNOS DATOS Y EJEMPLOS QUE EVIDENCIAN FRAUDES Y VIRUS

La última encuesta sobre hábitos de uso y seguridad de Internet de menores y jóvenes en España revela algunos datos en relación a este tema que hemos de tener en cuenta:

- **Uso de antivirus** El 82% de los equipos informáticos están protegidos con software antivirus.
- ***Configuración de perfil en redes sociales.*** El 53,1% de los usuarios de redes sociales tienen costumbre de configurar sus cuentas para que sólo sus contactos puedan acceder a sus perfiles.
- ***Uso de contraseñas.*** El 58,2% de los usuarios hace uso de las contraseñas para proteger sus equipos.
- ***Existencia de virus.*** El 22 % manifiesta haber sido infectado por un virus.
- ***Spam.*** El spam sigue siendo la incidencia más común que sufren los internautas (85%)
- ***Malware.*** Se ha detectado que alrededor de un 60% de los ordenadores están infectados de malware.
- ***Información a desconocidos***. Un 14,3% de las principales incidencias relacionadas con los menores se basan en haber facilitado información personal a desconocidos.
- ***Fraude electrónico***. El 48% de los usuarios ha sufrido alguna vez un intento de fraude electrónico.
- ***Datos personales.*** Existe un alto porcentaje de usuarios (44%) que tiene poca o ninguna confianza a la hora de facilitar sus datos personales mediante un e-mail o un servicio de mensajería instantánea.

A continuación vamos a ver algunos **ejemplos reales de infecciones de virus y fraudes o estafas**:

- La linterna molona

Se trataba de una aplicación que oficialmente ofrecía a los clientes de Android una linterna led para el teléfono, pero que una vez descargada permitía al desarrollador meterse en el terminal ajeno y enviar mensajes a números de tarificación elevada. En concreto, al aceptar las condiciones de uso –que se presentaban en una ilegible letra gris sobre fondo negro–, el usuario autorizaba al

Copyright 2026

fabricante a entrar en el dispositivo y enviar y borrar mensajes, tanto los que llegan como los que se mandan.

El programa publicaba automáticamente un post en la cuenta de Facebook de los usuarios que se lo descargaban. El post contaba las supuestas bondades de la app, un texto que todos los amigos del escritor inconsciente leían con gran entusiasmo creyendo que el autor había sido quien suscribía las líneas.

La aplicación fraudulenta se anunciaba como un programa que "hace brillar el led más que ninguna otra app de linternas y es totalmente gratuita", promesa que atrajo a miles de personas y que, por otro lado, en ningún caso se cumplía.

http://www.elconfidencial.com/espana/2015-03-05/medio-millon-de-estafados-por-una-app-linterna-que-se-suscribia-a-mensajes-premium-sin-autorizacion-del-usuario_722330/

- Vidas infinitas. Panda security descubre un estafa para el juego ‘Top Eleven Be a Football Manager’

PandaLabs han descubierto un malware en Windows que actúa disfrazado de aplicación. En teoría, si la descargamos podremos ganar tokens para el Football Manager con los que comprar jugadores.

Evidentemente, esto no sucede y, si lo que hacemos es seguir las instrucciones que nos dan, no solo no vamos a conseguir tokens gratis para Top Eleven sino que podremos perder el acceso a nuestra cuenta de correo electrónico o de Facebook.

La estafa para conseguir tokens gratis para el Top Eleven se hacía de la siguiente manera: 1º Te descargas esta app desde diferentes foros sobre juegos. 2º Para conseguir el número de tokens que selecciones tienes que insertar tu cuenta de correo electrónico o de Facebook, así como las contraseñas con las que accedes. Finalmente esos datos son enviados a los ciberdelincuentes que los utilizan para hacerse con el control de tu cuenta, impidiéndote el acceso a la misma.

http://www.pandasecurity.com/spain/mediacenter/noticias/estafa-para-top-eleven-football-manager/

- Estafas de falsos “amigos” en Facebook

Usted recibe una solicitud de amigo, pero no tiene tiempo de revisar esta nueva persona y pulsa ” aceptar ” de todos modos. O puede ser que la configuración de privacidad de su página está tan abierta y cualquiera puede verla. De cualquier manera, el estafador utiliza el acceso a su cuenta para ver las imágenes y otros datos de su perfil. Luego crea una nueva cuenta bajo su mismo

nombre y la llena de sus fotos, intereses y actualizaciones de estado. Con 500 millones de personas en Facebook en todo el mundo, es poco probable de detectar al impostor.

Después de crear una cuenta duplicada, el estafador envía solicitudes de amistad a sus amigos de Facebook. La gente reconoce su nombre y pulsa ” aceptar “, sin darse cuenta de que la cuenta es una falsificación. No se dan cuenta que algo anda mal hasta que su impostura comienza el envío de solicitudes de dinero y enlaces que son spam.

Los mensajes y los enlaces pueden ser estafas obvias cuando provenga de una dirección de correo electrónico desconocido, pero son mucho más creíbles cuando se comparte por un “amigo” de Facebook. ¡Siempre tenga cuidado con lo que haga clic, sin importar quién la comparte!

http://www.lafamiliadebroward.com/cuidado-con-las-estafas-de-falsos-amigos-en-facebook/

- El virus de la Policía ataca de nuevo al sistema Android

El virus de la policía es uno de los ransomwares más extendidos en los últimos años. Este virus, que está activo desde 2011, “secuestra” todos los archivos del ordenador, argumentando que el usuario ha estado navegando por páginas web pornográficas con contenido infantil, y pide “como multa” 100 € para liberar la información.

Hace varios días apareció una nueva familia de malware para Android, Android/Koler.A. Los medios se hicieron eco del mismo ya que era un ataque del tipo del “Virus de la Policía” / ransomware, parecido a los que hemos visto en ordenadores Windows, aunque en esta ocasión estaba dirigido a teléfonos móviles.

En este caso, el malware no es capaz de cifrar los datos del teléfono, pero aún así es bastante molesto y difícil de eliminar (si no cuentas con antivirus para Android) ya que el mensaje que muestra en pantalla está encima de todo lo demás y el usuario sólo dispone de unos pocos segundos para intentar desinstalarlo.

http://www.pandasecurity.com/spain/mediacenter/noticias/virus-policia-android/

3.3 Pautas y recomendaciones

PAUTAS Y RECOMENDACIONES PARA FAMILIAS Y EDUCADORES

Virus en Android: ¿cómo detectar si mi dispositivo está infectado?

Como bien sabemos, en Internet circulan infinidad de virus y malware que pueden poner nuestros equipos informáticos en riesgo, y precisamente en el caso de Android, en los últimos años han comenzado a proliferar notablemente este tipo de amenazas.

- Se abren anuncios y publicidad extraña
- El dispositivo funciona más lento de lo normal, deja de responder o se bloquea con frecuencia.
- Comportamiento extraño del dispositivo (se apaga solo aun teniendo batería).
- Las aplicaciones no funcionan correctamente.
- El antivirus se desactiva solo.
- Los programas se inician de forma espontánea.
- Creación de accesos directos a páginas no deseadas, es decir a servidores DNS falso.
- Aumento en el uso de datos

¿Qué podemos hacer si nuestro dispositivo está infectado?

Ante la sospecha de que nuestro ordenador o teléfono ha sido infectado por un virus, debemos reaccionar rápidamente y llevar a cabo las siguientes medidas siguiendo el consejo de especialistas como la que se encuentra en la revista Computer:

1º Controla los permisos de las aplicaciones

| Permisos | Concede | Niega | | --- | --- | --- | | Acceso a los ajustes | Sólo las apps de Google deberían pedirte este permiso, para asegurarse de que el dispositivo puede ejecutar todos los procesos que cada aplicación requiere. | Sólo las aplicaciones primarias de Google necesitan utilizar este permiso, así que si cualquier aplicación que requiera este permiso, desinstálala

Copyright 2026

enseguida. | | Modificación | La mayoría de las apps basadas en medios sociales usa esta función para guardar archivos en la tarjeta SD. Y sobre todo es muy común en las apps que usan vídeo. | Cualquier app con acceso a los contenidos de la tarjeta SD puede instalar un virus en ella. También pueden robar archivos o borrarlos de la tarjeta. | | Uso de la ubicación | Sólo suele ser importante para las apps de navegación tipo Google Maps. Otras aplicaciones quieren acceder a estos permisos para mostrar sitios de interés cercanos. | Las apps maliciosas pueden reunir información sobre tu ubicación y los lugares a los que vas, para enviarte anuncios basados en tu localización. | | ID del dispositivo e información de las llamadas | El principal uso de este permiso es leer el ID del teléfono y su estado, esto está bien cuando se accede a diferentes redes sociales o cuentas de correo electrónico. | Este permiso da acceso a tu número de teléfono, que podría ser utilizado por una aplicación maliciosa para enviarte spam constantemente. | | Hacer llamadas | Se trata de un permiso muy común para aplicaciones que permitan realizar llamadas de voz dentro de ellas, y que son independientes de la app Teléfono del dispositivo. | Hay aplicaciones que usan este permiso para marcar números de tarificación especial. Estas pueden ser de hasta 2 €/minuto. Así que cuidado. |

2. Tipo de infección. La mayoría de las infecciones en smartphones vendrán en forma de pop-ups, o un simple malware. Aunque no son muy perjudiciales para tu dispositivo, pueden ralentizar el rendimiento del teléfono o la tableta. Acude al cajón de aplicaciones para intentar encontrar cuál es la aplicación problemática.

3. Análisis antivirus. Incluso cuando creas que ya has identificado la aplicación problemática, haz un análisis antivirus completo del dispositivo. Descarga la aplicación Avast y selecciona la opción “Ejecutar análisis” disponible en la pantalla principal de la aplicación. Puedes escanear el dispositivo con un antivirus online. Aquí se muestran algunos:

- http://www.pandasecurity.com/spain/
- http://www.bitdefender.es/scanner/online/free.html
- http://www.zonavirus.com/antivirus-on-line/
- **Escanear el dispositivo con herramientas Anti Malware y AntiSpyWare**.
- **Desinstala aplicaciones problemáticas**.

Existen métodos avanzados de desinfección de virus que pueden realizarse sin llevar el dispositivo a un servicio técnico, pero requieren conocimientos avanzados de Informática, y pueden suponer un riesgo de pérdida de información si no se tiene claro lo que se está haciendo.

En la Oficina de Seguridad del Internauta se ofrecen instrucciones detalladas para llevar a cabo la desinfección, siempre bajo la responsabilidad del usuario.

http://www.osi.es/es/desinfecta-tu-ordenador

3.4 Estrategias de prevención

ESTRATEGIAS DE PREVENCIÓN EN EL HOGAR Y LOS CENTROS

Lo primero que debemos hacer las familias y tutores es informar a nuestros menores sobre cómo evitar este tipo infecciones de virus y fraudes. La buena comunicación es una de las claves fundamentales para la seguridad online..

Todas las precauciones son pocas para evitar infecciones de virus y para no ser víctima de un fraude electrónico.

A continuación se describen algunas recomendaciones técnicas a modo de prevención:

- ***Mantener actualizado todo el software instalado***, el sistema operativo, el navegador de Internet y antivirus: es fundamental contar con un antivirus actualizado en todos los dispositivos (ordenadores, tabletas y teléfonos móviles).
- ***Utilizar cuentas de usuario limitadas***: es aconsejable utilizar un usuario con permisos restringidos que no pueda instalar programas. De ese modo, si se cuela un virus, será más difícil que pueda instalarse.
- ***Realizar copias de seguridad***: las copias de seguridad permiten recuperar la información en caso de que un virus infecte un dispositivo, y deben realizarse en dispositivos externos (unidades de almacenamiento, discos duros, etc.).
- ***Realizar copias de seguridad en la nube*** (Cloud Computing): hacer copias de seguridad en la nube es una buena práctica que permite recuperar datos en caso de pérdida, pero no se deben hacer copias en la nube de información privada o confidencial, pues existe el riesgo de que esta información sea comprometida, ya que la información no suele estar cifrada (por ejemplo, Dropbox) y cualquier ciberdelincuente con acceso remoto al dispositivo puede acceder a la copia de seguridad.
- ***Gestión de contraseñas***: las contraseñas deben ser secretas, robustas y no repetidas. En este sentido, la Oficina de Seguridad del internauta ofrece varias técnicas para crear contraseñas robustas y seguras en el siguiente enlace: http://www.osi.es/es/contrasenas

- ***Verificar los enlaces cortos antes de acceder a ellos***: los enlaces cortos, empleados especialmente en pantallas móviles para ahorrar en caracteres, se configuran como un caldo de cultivo perfecto para ataques de phishing, ya que el usuario no sabe hacia dónde apunta el enlace. A modo de ejemplo, recomendamos el siguiente servicio para verificar enlaces desconocidos : www.unshort.me
- ***Evitar la navegación por páginas webs sospechosas*** (programas gratis, juegos gratis, fotos de famosas, etc.).
- ***Configurar adecuadamente la privacidad en las redes sociales***.
- ***Utilizar herramientas de Control Parental***. Pueden suponer una gran ayuda para los padres a la hora de evitar que los menores puedan verse involucrados en fraudes electrónicos e infecciones de virus.

Consejos sobre la instalación de aplicaciones en dispositivos móviles

- Descargar aplicaciones sólo desde fuentes confiables: Play Store para Android. Apple Store para IOS. Marketplace para Windows Phone.
- Sospechar ante un número bajo de descargas.
- Desconfiar si los comentarios son excesivamente halagadores, pues pueden estar escritos por el propio desarrollador o personas de su entorno.
- Comprobar los permisos de acceso al teléfono que se solicitan antes de iniciar la instalación. Por ejemplo, una aplicación de linterna no tiene sentido que requiera permisos para acceder al registro de llamadas.
- Desactivar en los dispositivos móviles la opción Permitir Orígenes Desconocidos ubicada en Ajustes > Seguridad > Orígenes desconocidos.
- Instalar un antivirus para dispositivos móviles.
- No utilizar navegadores extraños, ya que pueden contener vulnerabilidades que permitan “a los malos” robar las contraseñas.

Copyright 2026