# 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.

---

Revision #1
Created 1 February 2022 12:07:30 by Equipo CATEDU
Updated 1 February 2022 12:07:30 by Equipo CATEDU