PLAN DE SEGURIDAD USO DISPOSITIVOS MÓVILES.

"Evita la ocasión y evitarás el peligro".

1. Justificación.

El uso de dispositivos móviles ha incrementado exponencialmente entre todos los miembros de la comunidad educativa en los últimos cinco años, especialmente entre el alumnado de los últimos cursos de primaria. Así lo constatan las encuestas que hemos ido realizando durante estos años en el alumnado de nuestro propio centro. También en informe de UNICEF Niños en un mundo digital nos indica que el 71% de los jóvenes en edades comprendidas entre los 14 y los 25 años utilizan internet.

Cabe señalar que en muchas ocasiones los usuarios son completamente desconocedores del funcionamiento básico de los dispositivos digitales, como puede ser: configuración de seguridad, activación o desactivación de GPS, Bluetooth, acceso a redes, metadatos, copias de seguridad, actualizaciones, acceso al dispositivo, páginas web seguras, permisos de Apps instaladas, protección de datos…Todo un maremagnum de información que necesita de un plan de actuación, máxime si se trata de menores, centros educativos o empresas.

En esta noticia, sin ir más lejos, podremos leer cómo algunas aplicaciones infantiles sustraen información de menores como identificación, localización, nº de teléfono…

2. Objetivos.

Es fundamental plantearnos unos objetivos sencillos para comenzar nuestros plan y que sean fácilmente alcanzables, intentando huir de aspectos complicados que provocarán probablemente rechazo por una parte de usuarios.

General:

- Concienciar a los usuarios de la importancia de la seguridad.

Específicos:

- Aprender a configurar la seguridad de nuestros dispositivos.
- Utilizar contraseñas para proteger nuestros datos en red.
- Mantener nuestros equipos y apps actualizadas para reducir nuestra vulnerabilidad en red.
- Crear copias de seguridad para mantener seguros nuestros datos y aplicaciones.

3. Medidas del control del acceso al dispositivo.

- Es importante mantener nuestro dispositivo inaccesible a terceros utilizando algún tipo de medida de seguridad dependiendo del terminal que utilicemos, es decir, un **código de desbloqueo**, **reconocimiento facial** o **patrón de desbloqueo**. Tanto IOS como ANDROID disponen de **sensor de huellas dactilares** en algunos modelos.

- Las contraseñas mantienen a posibles intrusos alejados de nuestra información, al tiempo que protegen nuestro círculo más íntimo de posibles ataques, bien sea a través de chantajes o simplemente burlas.
- Recuerda: **“Evita la ocasión y evitarás el peligro”**. Esto se hace obligatorio en el caso de que manejemos datos como profesionales para cumplir con la LOPD
- Es importante señalar que el uso de un buen antivirus puede impedir que terceros accedan a nuestros dispositivos a través de malware o troyanos. Debemos ser cautelosos con la suplantación de identidad o phising que realizan algunos ciberdelincuentes así como los mecanismos de ingeniería social capaces de rastrear mucha información nuestra y de nuestros dispositivos.
- **¡CUIDADÍN! Especialmente con menores, son los más vulnerables**.
- A veces un gestor de contraseñas nos puede ayudar. EJ: Kee Pass.

4. Medidas de control de los datos compartidos.

- Los datos que almacenamos en nuestros dispositivos han de permanecer protegidos, para ello es importante que establezcamos las personas con las que los compartimos información así como eliminar o guardar en otros lugares aquellos archivos que ya no sean necesarios. Esta información es en muchas ocasiones “sensible” y si otros pueden tener acceso nos podemos convertir en potencialmente vulnerables.
- Es importante mantener desactivado el Bluetooth cuando no lo utilicemos.
- De igual manera es importante mantener desactivado el GPS.
- Si salimos de viaje, es importante no compartir fotos en redes sociales a tiempo real ya que podríamos estar compartiendo información sobre nosotros que nos pueda perjudicar. Los metadatos de las fotos también dan mucha información nuestra que nos puede convertir en vulnerables.
- Es fundamental leer las reseñas de otros usuarios antes de descargar aplicaciones, además de leer y sopesar condiciones.
- **Piénsate el sí quiero.**
- Es preferible utilizar conexiones 3G o 4G ya que son más seguras así como enchufar nuestros equipos a los dispositivos de otras personas siempre y cuando vayamos a acceder a información confidencial.
- Es importante no abrir enlaces que no se esperan y evitar spam. **“No piques. Nadie da duros a 4 pesetas”**.
- Actualizar contraseñas con asiduidad también nos evitará problemas.

5. Medidas de control remoto del dispositivo en caso de robo o pérdida.

- Es importante conocer las herramientas que utilizan tanto Android como Apple para localizar el dispositivo en caso de pérdida o robo así como para bloquear el acceso al teléfono. También las compañías que nos ofrecen los servicios de conexión a

internet, en sus aplicaciones nos permiten acceder al IMEI del teléfono, es decir, el código de nuestro terminal. Esto suele aparecer en ***"Productos contratados"***

- *también marcando desde nuestro teléfono *#06# y tecla de llamada.*

6. Sobre las actualizaciones del sistema o *apps*.

- Tanto el sistema operativo como las distintas aplicaciones están sometidos a constantes actualizaciones que mejoran el rendimiento de las mismas así como elevan nuestra seguridad. Es fundamental habituarse a realizar dichas acciones de forma rutinaria. Nos evitará algún disgusto innecesario de nuevo.

7. Copia de seguridad: cómo y cuándo se realizará.

Dependiendo del dispositivo realizaremos una copia de seguridad o "backup" para tener guardada nuestra configuración y poder acceder a ella en caso de pérdida o robo, así podremos recuperar toda la información relevante. Es conveniente realizarla quincenalmente como mínimo.

Los dispositivos android ofrecen GOOGLE DRIVE como almacén para dicha copia.
Por otro lado, en IOS tenemos ICLOUD que también permite dicha copia.
Es importante, dependiendo de cada caso, realizar copias de seguridad con cierta frecuencia puesto que nos ahorrará más de un disgusto.

En nuestro Blog de aula "Pick English With TICs" tenemos abundante información sobre el uso internet por parte de menores siguiendo la etiqueta Internet en el propio blog.

Bibliografía

Niños en un mundo digital UNICEF

Medidas de seguridad LOPD para dispositivos móviles

YOUTUBE Chema Alonso, ¿sabes lo que pasa cuando das a sí, acepto en una app?

Roban datos de menores a través de apps infantiles

Política de contraseñas y seguridad de la información

Evento en directo NOOC Seguridad en dispositivos móviles YouTube

Smartphones y tabletas

Protege tu móvil: Revisa los permisos de tus Apps

Privacidad y seguridad en internet

Javier Sellers Cerdá. @javiersellers71
Maestro de primaria especialista en inglés
Coordinador TIC
Colegio Santo Domingo Savio.
Petrer
Alicante