Seguridad en línea con SANGO

Glosario

Suplantación de identidad (phishing): La suplantación de identidad es un ataque de ciberseguridad que se realiza por correo electrónico y permite el robo de información personal gracias a la inserción de enlaces falsos en los mensajes para robar la contraseña o instalar un fichero con programas maliciosos.
Programa malicioso (malware): programa que daña los dispositivos electrónicos (computadora, tableta, teléfono inteligente).
Control parental: herramienta de protección que defiende a los niños de las amenazas en línea, e impide acciones que pueden resultar peligrosas.

Datos personales

- Cuando estamos en Internet no nos damos cuenta de la cantidad de **datos personales** que facilitamos ni de cómo pueden utilizarlos sin nuestro permiso.
- **Nunca des** tu **contraseña, domicilio, número de teléfono o fecha de nacimiento**.
- Pero tampoco te olvides de que ¡tus **aficiones** también son información privada! Ten cuidado con las fotos y los vídeos que publiques.
- **Nunca te olvides de que: ¡No hay nada en línea que sea totalmente privado!**

Aplicaciones

- Las aplicaciones **registran una serie de información personal tal como tus contactos y tus ubicaciones, lo que permite que alguien con malas intenciones** se entere de dónde te encuentras y cuándo utilizas la aplicación.
- **Consúltale siempre a una persona mayor** antes de comprar aplicaciones o desbloquear nuevos niveles de los juegos, para evitar situaciones indeseables.
- Cuando utilices aplicaciones o visites sitios web adecuados para tu edad, **juega exclusivamente con los amigos que conozcas personalmente**.

Redes sociales

- **Las redes sociales** son herramientas que se utilizan para **mantenerse en contacto con los amigos**, pero pueden albergar muchos peligros. De hecho, es realmente fácil crear un **perfil falso**: ten cuidado porque ¡**no tienes ni idea de quién podría ocultarse** detrás de un nombre de usuario!
- Además de entrar en contacto con personas malintencionadas, es posible que recibas **contenidos inadecuados para tu edad**, tales como fotos y vídeos, que puede que te hagan sentirte **incómodo**.

Peligros

- Robo de datos.
- Robo de identidad.
- Suplantación de identidad (phishing).
- Ver fotos o vídeos inadecuados para tu edad.
- Las aplicaciones siempre se enteran de dónde te encuentras si tu "ubicación" está activada.
- Tus contenidos personales pueden divulgarse sin tu permiso.

¡SABÍAS QUE...
Tu teléfono inteligente también guarda tu información personal, así que ¡déjalo siempre bloqueado, y cuídalo!

¿Qué puedes hacer para protegerte cuando estás en línea?

Deja siempre bloqueado tu dispositivo cuando no lo estés utilizando y emplea contraseñas largas, complejas y secretas para proteger todas tus cuentas.

Configura tu perfil como privado, nunca le des tu información personal a nadie y, si es necesario, utiliza un alias.

Asegúrate de que conoces personalmente a los amigos con los que te relacionas en los chats y las redes sociales: comparte exclusivamente contenidos con los que te sientas cómodo.

Si recibes peticiones o contenidos que te hagan sentirte incómodo o ves algo que no sea adecuado para tu edad, cuéntaselo a una persona mayor.

Pídele a alguna persona mayor de tu confianza que configure el Control Parental en los dispositivos que utilices.

Sigue atento y mantente informado en:
www.itu-cop-guidelines.com y www.itu.int/cop

eni Deloitte. ITU