Digipadres

UNA INICIATIVA DE saferkidsonline by eset

Zoom y cámaras web: cómo proteger la privacidad de los menores

El Zoom, Meet, Teams y otras aplicaciones similares son tendencia hace años, pero después del 2020 la mayoría de los niños (y los padres) debieron adaptarse bruscamente a una nueva realidad donde las videollamadas son parte del día a día. Por eso, es más importante que nunca cuidar tanto nuestra ciberseguridad como la de los niños.

Uno de los cambios más drásticos que trajo la pandemia fue sin dudas el paso abrupto a la virtualidad en la mayoría de los ámbitos de la vida: el trabajo, el colegio, actividades recreativas y más. En 2021 todavía se está intentando definir qué hacer con todo esto mientras se instaura una nueva normalidad.

Como sabemos que estos cambios pueden ser abrumadores, desde ESET queremos recordarles a todos los digipadres algunos consejos para cuidar la seguridad de los niños al utilizar dispositivos electrónicos y la aplicación Zoom para acudir a sus clases u otras actividades.

Las formas más comunes de acoso en Internet

Utilizando códigos maliciosos, **los ciberdelincuentes pueden intentar comprometer un dispositivo, obteniendo acceso a su cámara o micrófono sin el consentimiento de las víctimas, espiando los aspectos más íntimos de sus vidas (spyware)**. Las motivaciones varían: algunos encuentran emocionante la idea de ver a alguien en secreto, otros buscan extorsionar a sus víctimas amenazando con publicar esos videos si no reciben dinero.

Nuestras recomendaciones para cuidar a los niños de esta amenaza son:

» Enseñarles a los niños a cubrir sus cámaras siempre que no las estén usando.
» Asegurarse de que la configuración por defecto de la cámara web siempre sea "apagada".
» Utilizar soluciones de seguridad capaces de proteger las cámaras a nivel software.
» Educar a los niños para que no hagan nada fren-

te a una cámara web descubierta que no harían si alguien estuviera mirando.

» Dar el ejemplo: cubrir las cámaras de toda la familia.

Configurar la seguridad de la plataforma de videollamada que se utilice

Como ya dijimos el cambio a la virtualidad nos afectó a todos, **y las plataformas de videollamadas no estuvieron exentas de sufrir brechas de ciberseguridad, hackeos, filtraciones de datos, entre otras**. Por eso es importante configurarlas desde casa para tratar de reducir al máximo los riesgos de quedar involucrados en estos ataques.

» Asegurarse de que las llamadas sean privadas y que solo se pueda acceder con contraseña o link para evitar intrusos en ellas.

» Iniciar las reuniones siempre con cámara apagada y, si es obligatorio, prenderlas asegurándose de cambiar el fondo, haciendo que se vea borroso o usando un fondo predeterminado de Zoom para evitar que se revele información personal de forma involuntaria.

» Educar a los niños para que no compartan (ni por escrito ni en diálogo) información personal o confidencial.

» Activar el doble factor de autenticación (2FA). Zoom agregó a finales de 2020 esta posibilidad y siempre es una gran forma de agregar una capa de seguridad a las videollamadas.

Descargar aplicaciones oficiales y siempre actualizarlas

Las aplicaciones de mensajería, videollamadas, o incluso juegos, deben ser siempre descargadas desde la tienda oficial de aplicaciones del móvil o desde la PC o laptop. Si se descargan en otros sitios no oficiales, puede suceder que sean aplicaciones falsas o con malware que infecten los dispositivos.

Luego de descargarlas, es importante actualizarlas apenas se lanza la nueva versión. Esto es así porque con cada actualización se reparan vulnerabilidades con parches o surgen nuevas funciones o capas de seguridad que es importante incorporar en nuestros equipos para evitar ataques.

Usar soluciones de Control Parental para cuidar a nuestros hijos mientras ellos disfrutan

Luego de tener clases, ya sean virtuales o presenciales, es muy probable que los niños quieran en algún momento utilizar dispositivos electrónicos para jugar, publicar en las redes sociales o simplemente distraerse. Esto es algo común en la nueva normalidad y sucede cada vez con mayor frecuencia. **Por eso es importante, además de educarlos en ciberseguridad, contar con una solución de seguridad con Control Parental como puede ser ESET Parental Control para Android.** Esta solución evita ataques de ciberdelincuentes, bloquea los sitios inapropiados para ellos, apaga los dispositivos en automático tras un tiempo determinado de utilización, entre otras funciones clave para evitar que los niños pasen por situaciones desagradables.

¡Con estas recomendaciones ya estamos listos para que nuestros niños participen en clases, jueguen y hablen con sus amigos de forma segura!

Queremos que más **Digipadres** potencien a los niños
y les enseñen a navegar seguros.

¿Estás listo para acompañarnos en este desafío?

www.digipadres.com

eset