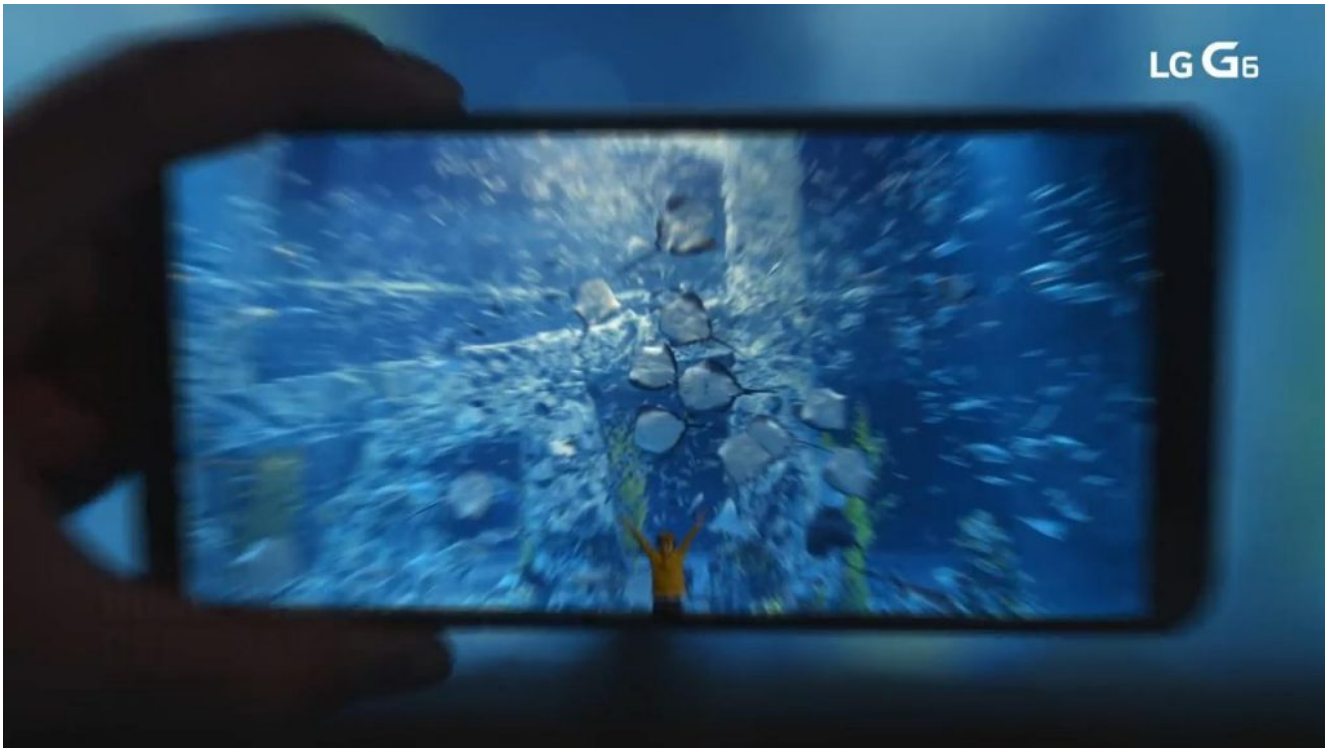

El 16% de los niños tiene su primer smartphone antes de los 10 años

El 16% de los niños tiene su primer smartphone antes de los diez años y el 22% de los menores comprendidos en esta franja de edad ya tiene perfil en redes sociales, según se desprende de un estudio de realizado por S2 Grupo, que señala que la formación y la concienciación sobre el uso seguro de las nuevas tecnologías sigue siendo una «tarea pendiente» para evitar ser víctimas de ciberdelincuentes, especialmente entre menores y jóvenes, pero también en el ámbito empresarial.

Con motivo de la celebración este martes 6 de febrero del Día Internacional de la Internet Segura, expertos de S2 Grupo han advertido de que «el aumento en el uso de las Nuevas Tecnologías por parte de los menores y cada vez a edades más tempranas, hace esencial incrementar la concienciación sobre su uso seguro para evitar que sean víctimas de ciberdelincuentes o ellos mismos incurran en delitos por no utilizarlos adecuadamente».

Según una encuesta realizada por la compañía a través de su blog

Hijosdigitales.es el 16% de los padres aseguraban haber comprado su primer smartphone a sus hijos antes de los 10 años y que el 22% de los menores, incluidos en esta franja de edad, ya utilizan redes sociales.

> *El 16% de los niños tiene su primer smartphone antes de los diez años y el 22% de los menores comprendidos en esta franja de edad ya tiene perfil en redes sociales*

«Los problemas originados en entornos conectados son múltiples y la tendencia indica que seguirán aumentando, eso hace que se disparen las alarmas y que desde tanto las instituciones públicas, organizaciones y entidades privadas nos pongamos en marcha para formar y concienciar a los menores y evitar que sean víctimas de delitos relacionados con el uso de las Nuevas Tecnologías», ha explicado José Rosell, socio-director de S2 Grupo.

El ciber acoso, el sexting, la pérdida de privacidad, las adicciones o las apuestas online son sólo algunos de los riesgos a los que pueden enfrentarse los menores relacionados con este ámbito, ha señalado Rosell.

«Muchas familias piensan que limitar el uso de estas tecnologías es la solución para evitar ciberproblemas, pero esto es inútil. Los dispositivos conectados están cada vez más implantados en cada ámbito de nuestra vida y la auténtica forma de protegernos es conocer los riesgos a los que nos enfrentamos y cómo realizar un uso responsable de Internet», ha apuntado.

DECÁLOGO PARA USO RESPONSABLE DE NUEVAS TECNOLOGÍAS

Para promover un uso responsable de las Nuevas Tecnologías, expertos de S2 Grupo han elaborado un decálogo de 'consejos clave' para que la experiencia sea más segura. En primer lugar recomiendan a los padres aprender a utilizar la misma tecnología que sus hijos. Si éstos desconocen los entornos en los que se mueven sus hijos se crea una gran distancia entre ambos que se traduce en falta de autoridad, alertan.

Además, aconsejan utilizar contraseñas robustas –con letras mayúsculas y minúsculas, signos de puntuación y caracteres alfanuméricos–, modificarlas con frecuencia y ser diferentes para cada entorno.

No hay que aceptar a extraños como amigos en Redes Sociales. «Esto puede entrañar un grave peligro para los menores, que no saben si en realidad detrás de los perfiles hay gente de su edad o adultos con algún tipo de intención perniciosa».

Los expertos avisan de la necesidad de proteger la webcam. Si un ordenador es hackeado, la cámara puede ser activada por control remoto aunque parezca que está apagado. Si encima el dispositivo está en la habitación del menor podrían tomarse imágenes íntimas, desnudo, etc., advierten.

Advierten de no enviar fotos íntimas, cosa que puede acabar en situaciones altamente delicadas como el chantaje o el acoso; tener cuidado con lo que se comparte y no estar continuamente informando, por ejemplo, de dónde nos encontramos, dónde vamos, si estamos de viaje, etc.

La mejor medida de protección es la educación: conocer los riesgos y cómo protegerse es una de las mejores herramientas para evitar ciberpeligros, agregan.

Tampoco recomiendan utilizar wifis públicas, que no suelen garantizar la seguridad suficiente y muchas son realmente «cebos» de ciberdelincuentes para hacerse con el control de nuestro smartphone y tener acceso a toda nuestra información.

A la hora de configurar la privacidad de las cuentas en las Redes Sociales es fundamental escoger la opción más restrictiva para evitar que personas no deseadas accedan a nuestros datos. Finalmente, para evitar que los dispositivos sean hackeados, es importante que el navegador, el sistema operativo y el antivirus estén correctamente actualizados

PRINCIPAL RIESGO: EL DESCONOCIMIENTO

El proyecto ProtectIT de S2 Grupo es un programa dirigido a organizaciones en el que se trabaja con todos sus miembros y familias para conseguir una cultura eficaz de la seguridad en ellas. El objetivo es incrementar el nivel global de la ciberseguridad y disminuir el riesgo de incidentes relacionados directamente con uno de los componentes clave en esta materia que son, precisamente, las personas.

Para ello, entre otras medidas, se presenta a los participantes situaciones

impactantes pero cotidianas, que llaman su atención sobre comportamientos de riesgo, sus consecuencias y la influencia que éstos tienen sobre la ciberseguridad.

Según S2 Grupo, el principal aspecto que hace que las familias se sitúen en riesgo es «el desconocimiento de las amenazas a las que se enfrentan en el ámbito digital». Tanto los adultos como los menores no tienen consciencia de ésta y, por tanto, no gestionan los riesgos asociados. Estos peligros se derivan tanto de las vulnerabilidades técnicas asociadas al uso de los dispositivos y al acceso a servicios online como de prácticas de comportamiento inseguro, principalmente por parte de los menores.

En 2017, S2 Grupo a través del programa ProtectIT contribuyó a concienciar a más de 10.000 empleados y 1.000 familias. Realizó más de 150 sesiones presenciales en empresas para la divulgación de la importancia de una cultura de la seguridad en cualquier entidad, ya sean grandes compañías del Íbex35, por ejemplo, o pymes. De éstas, 75 sesiones se realizaron con empleados, más de 20 con equipos de alta dirección y más de 20 fueron jornadas familiares de seguridad. También se realizaron más de 10 acciones específicas de coaching individualizado para altos cargos.