El error de dejar un móvil viejo a tus hijos para jugar y poco más... se lo pones muy fácil a los ciberdelincuentes

J. C. CASTILLO

Cerca del 70% de los menores españoles de entre 10 y 15 años cuentan con un smartphone a libre disposición, según la última 'Encuesta sobre Equipamiento y Uso de Tecnologías de la Información y Comunicación en los Hogares' del Instituto Nacional de Estadística (INE). De hecho, el acceso de los niños a la tecnología arranca incluso antes, siendo habitual que los padres les endosen una tableta electrónica (o sus propios móviles) para tenerlos entretenidos tanto dentro como fuera de casa.

No es de extrañar, en este contexto, que los ciberdelincuentes estén cada vez más interesados en dicho segmento de usuarios: el robo de identidades de menores se ha disparado en el último lustro (según dejan entrever las cifras publicadas por Javelin Strategy), muchas veces fruto del ingente número de aplicaciones maliciosas disponibles (clones de juegos gratuitos, apps educativas...).

«Los niños y los adolescentes son el eslabón más débil de la cadena digital de la familia –explica Jonay Puente, docente del Máster de Ciberseguridad de IMF Business School–. Instalan mil juegos y apps, hacen clic en todo y suelen tener menos formación en seguridad. Además, muchas veces los padres usan en esos dispositivos sus propias cuentas de correo, de compra o de trabajo. Eso convierte el móvil del niño en una puerta de entrada a datos de toda la familia e incluso de la empresa del adulto».

Otra razón de peso para que los malhechores digitales se fijen en los menores, prosigue Puente, es que reaccionan peor a la presión: «Si un delincuente les amenaza con publicar fotos o mensajes privados, es más fácil que consigan que paguen o que den más datos. Y todo esto con un plus importante: suele haber menos control técnico, con dispositivos sin protección y con contraseñas muy débiles».

Respecto a las amenazas o fraudes más comunes a que están expuestos nuestros hijos, el experto incide en los engaños que juegan con la curiosidad o el deseo de conseguir cosas gratis: «Entran por mensajes en redes, chats de juegos o correo que prometen monedas del juego, trucos, premios o acceso anticipado a contenido. Ahí meten enlaces que llevan a páginas falsas para robar cuentas o que descargan malware. También se ve mucho la suplantación de identidad con perfiles falsos que se hacen pasar por amigos, famosos o incluso profes. A partir de ahí piden fotos, datos personales o intentan mover al menor a otras plataformas con menos control. Y no hay que olvidar las apps que piden permisos exagerados y acaban recopilando más información de la que deberían».

Consecuencias de la dejadez paterna

Qué duda cabe de que la supervisión paterna contrarrestaría buena parte de los peligros descritos. La realidad, sin embargo, evidencia un exceso de confianza altamente perjudicial: «Los padres piensan que si le regalan o ceden a sus hijos un móvil barato, solo para juegos, nadie querrá atacarlo. Es justo al contrario: un dispositivo viejo sin actualizar es justo el objetivo perfecto», expone el docente de IMF.

«Otro clásico es creer que con instalar una única app de control parental ya está todo hecho, cuando esa app no sustituye la educación básica en materia de seguridad digital. Muchos dan por hecho que en el colegio o el instituto ya les han enseñado todo lo que necesitan saber y, a veces, solo han recibido una charla muy general», motivo este último por el que Puente recomienda encarecidamente a los padres que instruyan a sus hijos sobre cómo reconocer comportamientos o mensajes sospechosos en Internet: «Lo mejor es traducir la ciberseguridad a normas sencillas y repetidas muchas veces. Por ejemplo, nadie que sea de confianza te pide contraseñas, códigos o fotos íntimas por chat. Si alguien te mete prisa, te amenaza o te regala algo demasiado bueno para ser verdad, se considera sospechoso y se enseña al niño a parar y a pedir ayuda antes de hacer clic».

También ayuda practicar con ejemplos, añade: «Enseñar pantallazos de mensajes trampa, jugar a adivinar qué está mal, explicar por qué una dirección web es rara o por qué esa cuenta parece falsa. Y muy importante, dejar claro que no se les va a reñir por contar algo raro que hayan visto. Si tienen miedo a la bronca, ocultarán justo lo que los padres necesitan saber».

Señales de alerta y precauciones a tomar

Firmas especializadas en ciberseguridad como Kaspersky recomiendan adelantarnos a todo mal sacando partido a las herramientas y opciones que incluyen, por defecto, la mayoría de dispositivos. En un móvil Android siempre es buena idea configurar una cuenta familiar de Google, mientras que en un iPhone acudiremos al apartado 'Tiempo de uso' del menú de 'Ajustes' para fijar horarios permitidos y restringir el acceso a determinadas aplicaciones.

A lo anterior podemos sumar «la creación de usuarios específicos para los niños en el ordenador familiar (activando previamente los respectivos controles del sistema); y la configuración del router doméstico para filtrar contenidos y programar horarios de conexión», sentencia Puente, quien enumera al tiempo las señales de que el dispositivo de nuestro hijo ha sido comprometido: «Las pistas típicas son un móvil que va mucho más lento de lo normal, la batería que se agota con rapidez, la aparición de ventanas emergentes extrañas o aplicaciones que nadie recuerda haber instalado; los mensajes que llegan a padres o amigos que el menor dice no haber enviado, las compras no autorizadas en juegos o los inicios de sesión sospechosos en cuentas del niño».

Ante cualquiera de estos 'síntomas', los expertos recomiendan desconectar el aparato de Internet y pedir al menor que no lo use hasta restaurarlo de fábrica; cambiar las contraseñas de todas las cuentas importantes (desde otro dispositivo), revisar el extracto del banco en busca de transacciones sospechosas y guardar capturas que evidencien cualquier intento de chantaje o acoso. Casos estos últimos que no dudaremos en comunicar tanto al centro educativo del niño como a las autoridades.