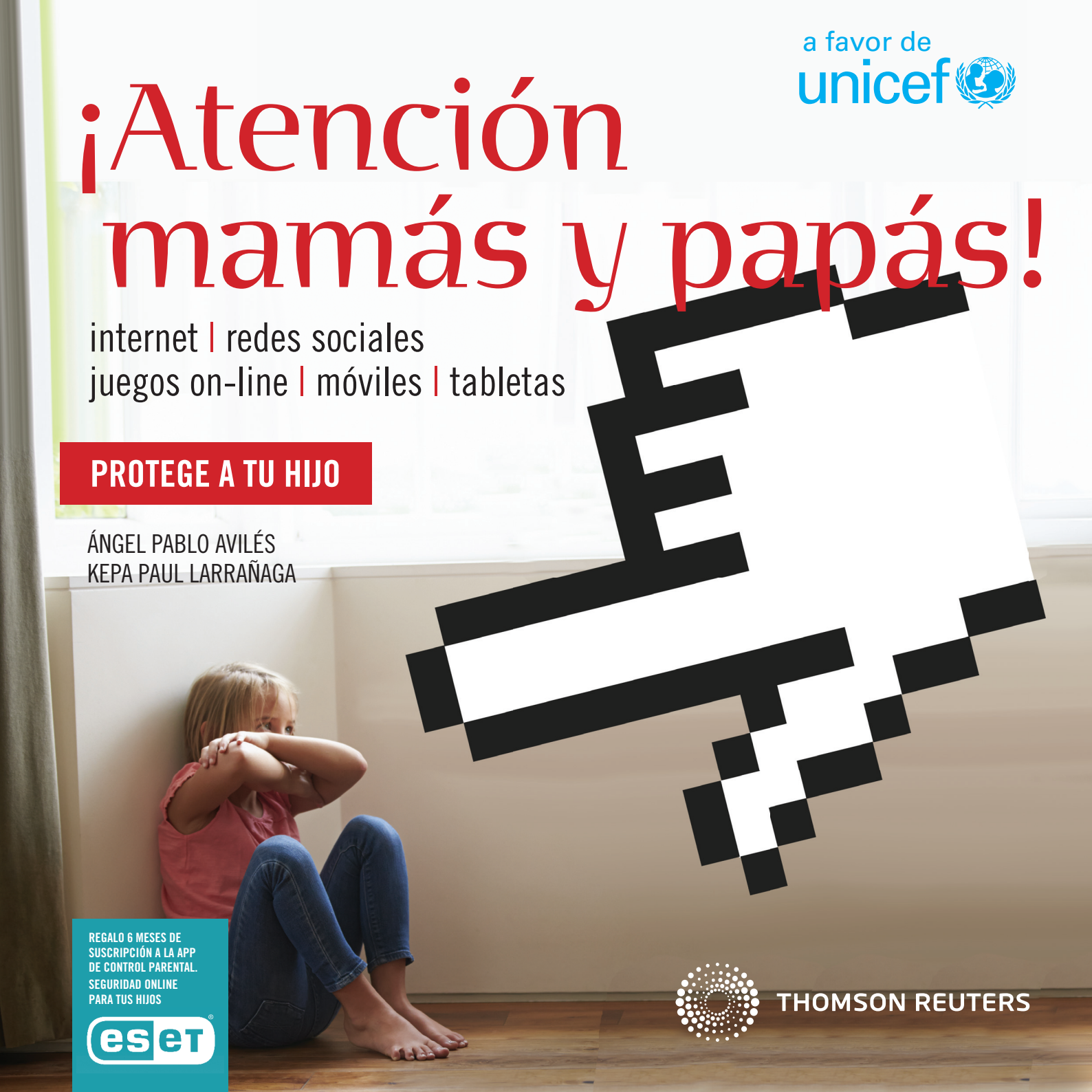
a favor de unicef

¡Atención mamás y papás!

internet | redes sociales
juegos on-line | móviles | tabletas

PROTEGE A TU HIJO

ÁNGEL PABLO AVILÉS
KEPA PAUL LARRAÑAGA



THOMSON REUTERS

Resumen

Esta **guía práctica** da respuestas rápidas y concretas a vosotros, padres y madres, con **hijos e hijas usuarios de dispositivos móviles:** Smartphones, Tablets y Wearables. Ofreciendo **60 casos sobre situaciones de uso posibles** de dispositivos móviles por niños, niñas y adolescentes, y analizadas sobre los tres espacios donde habitan éstos: **la familia, la calle y la escuela o instituto.**

Dos expertos en seguridad tecnológica y en educación en derechos de infancia y en TIC (Tecnologías de la Información y de la Comunicación) analizan de manera pormenorizada los distintos casos incluyendo testimonios y soluciones, y dando un **doble enfoque desde la seguridad** y de la **educación**.

Contiene distintas infografías sobre aspectos de uso práctico y **dos diccionarios:** uno de mensajería instantánea y otro de emoticonos.

Ventajas

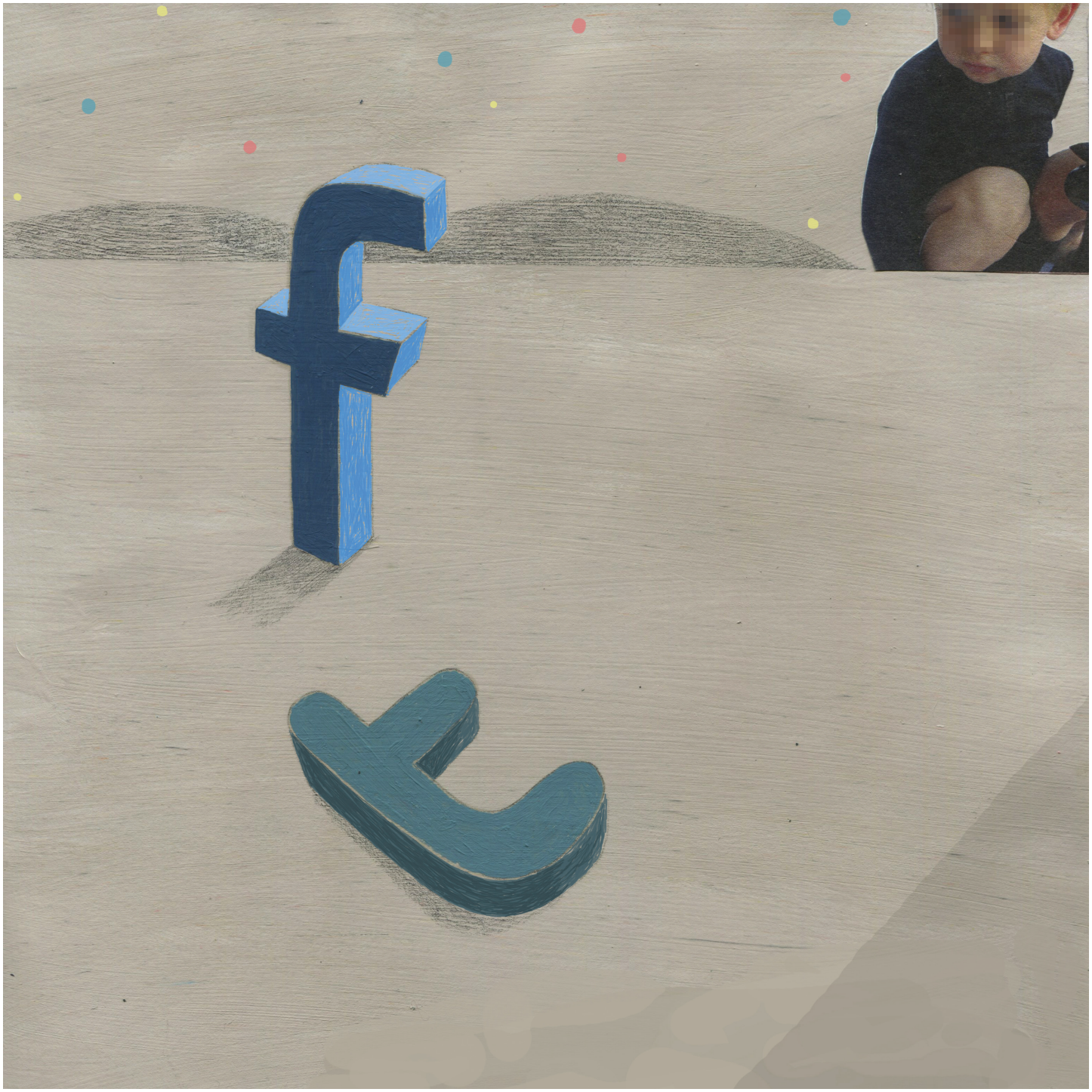
Incluye acceso a la **APP de seguridad** online "ESET Control Parental para Android". 6 meses de suscripción gratuita a esta aplicación que garantiza la seguridad online de tus hijos.

Control de aplicaciones e Internet, límite de tiempo en juegos, control de ubicación...

Colabora

Por la compra de cada guía, se destina **1€ a favor de:**

unicef



01 LA SEGURIDAD DE LAS CONTRASEÑAS Y DE COMPARTIRLAS CON TERCERAS PERSONAS

Un adolescente para mostrar fidelidad con sus amigos o con su pareja comparte con éstos sus contraseñas de acceso a sus cuentas personales y a las redes sociales. El acceso a las cuentas o redes sociales de otra persona, sabiendo usuario y contraseña, se puede hacer desde cualquier tipo de dispositivo móvil que se disponga con conexión a Internet, y por lo tanto en cualquier momento o lugar.

"Tuve que dar para demostrar fidelidad a mi novio mis contraseñas. Acepté, y ahora tras cortar con él, me arrepiento pues aunque he cambiado, por supuesto, las contraseñas, se hizo con fotos e información personal, utilizándola en mi contra".

" Mi contraseña es muy sencilla y por eso la utilizo para todos mis perfiles, "1234", ¡jamás se me va a olvidar!"

1. Acceso a los perfiles, por terceras personas, ante contraseñas débiles o predecibles.
2. Amenazas de hacer viral la información obtenida de los accesos.
3. Sufrir el robo de *identidad digital* desde los propios perfiles de redes sociales y/o cuentas de correo vulnerables.

1. Poder hablar esta situación con la ex-pareja o examigo para acordar y pactar que no use en tu contra la información: fotos, vídeos y conversaciones privadas.
2. Que sea sólo un arrebato pasajero a causa de la ruptura, y siendo las intenciones de la ex-pareja buenas.

Las contraseñas en Internet son como las llaves de nuestra casa, no se deben compartir con nadie. En este supuesto las llaves de casa las tienen los componentes adultos de la familia y los menores a partir del momento que se considera que tienen la suficiente responsabilidad para custodiar algo tan importante como es el acceso a nuestro hogar.

Pesa mucho la influencia de la comunidad de amigos, en la infancia y en la adolescencia. reforzada por ser más intensas las relaciones con las redes sociales de Internet, y el uso de servicios de *mensajería instantánea*. Al estar tan comprometidos dan prioridad siempre a la fidelidad al grupo o la pareja.

De la misma manera, por esta misma razón de compartir con la comunidad, puede ocurrir que la información personal llegue a terceros desconocidos con malas intenciones.

1. Las contraseñas son personales, y no deben de ser compartidas con nadie, salvo, por seguridad, con los padres.
2. Una contraseña debe de ser, fácil de recordar y difícil de olvidar, será alfanumérica y contendrá algún carácter especial, estará compuesta por al menos 8 caracteres.
3. Una contraseña debe ser exclusiva para cada servicio. Cada uno de nuestros perfiles en la red dispondrá de una contraseña distinta.

1. Es necesario fomentar el diálogo entre niños y adolescentes sobre seguridad informática. Inculcando las razones y motivos de una mala práctica en el uso de las TIC. No solo a nivel personal sino de qué manera puede afectar al grupo de amigos si un desconocido accede a las cuentas personales tras difundirse sus contraseñas, pues son sus contactos.
2. La seguridad y privacidad en el uso de las TIC es una materia de aplicabilidad práctica, y posible asignatura escolar, que afecta a todos, al estar interconectados siempre con los dispositivos móviles.

¿Cómo es posible tener una contraseña alfanumérica, con caracteres especiales y números, que además sea única y fácil de recordar?

¿Es necesario fomentar el diálogo entre niños y adolescentes sobre su privacidad en Internet?

¿Son necesarias asignaturas concretas en la escuela para tratar cuestiones relacionadas con la seguridad y *vida digital*?

SUMARIO

Situaciones en espacio de calle o tránsito

31. Tener activado el GPS en los dispositivos móviles.
32. Conexión a una red wifi en tránsito.
33. Usar un dispositivo móvil de un amigo.
34. Etiquetar fotos sin permiso.
35. Monitorización de datos mediante 'Wearables'.
36. Publicar 'selfies' en las redes sociales.
37. Pulsar 'Aceptar' sin leer las condiciones de instalación de una aplicación.
38. Compartir información y datos personales a terceros sin querer.
39. Robo o pérdida del dispositivo móvil.
40. Recepción de mensajes anónimos, para obtener información del receptor.

Infografía 5.- ¿Cómo proteger nuestra Privacidad con los dispositivos móviles?

41. Querer tener más amigos que otros en las redes sociales.
42. Atender de manera continuada las redes sociales.
43. Dejar a los hijos usar los dispositivos móviles de los padres.
44. No proteger el acceso al dispositivo móvil con contraseña.
45. Escanear Códigos QR expuestos en la calle.
46. Ejercer violencia de género utilizando las redes sociales.
47. Atacar o agredir a alguien para grabarlo en vídeo.

Infografía 6.- ¿Cómo detener la Sincronización en los dispositivos móviles?

Situaciones en el espacio escolar

48. Ser espectador del ciberacoso escolar mediante las TIC.
49. Sufrir una agresión grabada dentro del recinto escolar.
50. Uso inapropiado del wifi de la escuela o instituto.
51. Conectar con Bluetooth 'Wearables' y dispositivos móviles para copiar en exámenes.
52. Distribuir fotos/vídeos de 'sexting' entre terceros en el centro educativo.

Infografía 7.- ¿Qué retios hay en el Patio del colegio?

53. Utilizar el 'Dispositivo móvil' dentro del aula.
54. Utilización de 'Smartwatch' dentro del aula.
55. Grabar en vídeo o fotografiar a un profesor en el aula.
56. Práctica de 'cyberbullying' entre niños y adolescentes.

Infografía 8.- ¿Qué retos hay en el Aula del colegio?

57. Uso de 'nicks' o pseudónimos en las cuentas personales.
58. Realización de tareas escolares en la nube (cloud).
59. Uso de plataformas virtuales en la escuela o Instituto.
60. Prestar atención a varias tareas, a la vez que se consulta en un dispositivo móvil.

Infografía 9.- El reto de la Competencia digital.

THOMSON REUTERS