Digipadres

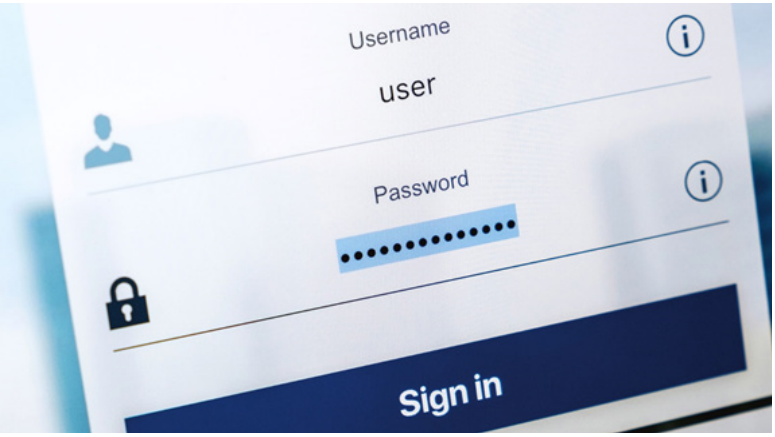
UNA INICIATIVA DE ESET

Contraseñas fuertes para cuidar los perfiles y apps digitales

¿Cuál es la contraseña más simple que te viene a la mente? ¿"1234", "contraseña", "qwerty"? Hoy en día, los niños suelen usar códigos similares, ya que valoran más la comodidad que la seguridad. Y dado que necesitan un nombre de usuario y una contraseña para cada servicio online al que se unen, a menudo terminan reutilizando las mismas contraseñas en distintas cuentas.

Lamentablemente, el hecho de tener una contraseña fácil de adivinar puede generar una serie de problemas. Por ejemplo, les aconsejamos a nuestros hijos que ahorren dinero, pero *¿qué pasa si alguien más logra acceder a su aplicación bancaria? ¿Qué pasa si alguien hackea sus cuentas de redes sociales e inicia una campaña de odio?* Hay innumerables aplicaciones que requieren acceso a las imágenes y a la ubicación del dispositivo. Esto podría suponer un grave riesgo para la seguridad de los menores.

Tanto padres como madres, al ser sus consejeros de mayor confianza, deben estar presentes para ayudarles a crear su primera contraseña fuerte. Para ello es necesario que les expliquen las mejores prácticas y resalten su importancia.



A continuación, mostramos algunos consejos para crear una buena contraseña:

1. Es única. Cada cuenta debe tener su propia contraseña.

2. Es larga. El largo mínimo recomendado es de ocho caracteres, pero cuanto más larga sea la contraseña, mejor. Los delincuentes de hoy son capaces de adivinar cuatro caracteres o números al azar en pocos segundos. Por eso, para mejorar la seguridad del código secreto, hay que añadir más caracteres de distintos grupos.

3. Como puede ser difícil de recordar, conviene **usar una frase de contraseña**, es decir, una oración breve o un dicho que sea fácil de recordar. Las frases de contraseña suelen ser mucho más largas que una contraseña básica que sólo combina una cantidad limitada de caracteres y números diferentes, y por lo tanto protegen mejor las cuentas.

4. Tiene algunas de sus letras reemplazadas por caracteres especiales (@, #, $, etc.) o números para que sea más difícil de adivinar.

5. Evita palabras de uso común, como "contraseña", "secreto", así como el nombre del niño, los padres, hermanos o mascotas, que a menudo se pueden encontrar en las redes sociales.

6. Evita los caracteres repetitivos y secuenciales, como "1111", "1234" o "abab".

7. Es secreta. Aunque este punto es importante, es útil sobre todo para niño/as mayores y adultos. Los más pequeños, en cambio, pueden olvidar las contraseñas y todavía necesitan la orientación de un adulto cuando navegan por Internet. Por eso, en este caso resultan muy útiles las cuentas compartidas entre adultos e hijos o las aplicaciones de control parental.

Una forma divertida de aprender a crear contraseñas fuertes

Si tienes **adolescentes** en casa, puedes invitarlos a participar de una **competencia familiar** para calificar sus contraseñas. En la primera ronda del juego, cada participante escribe sus propias contraseñas en una tarjeta y las pega en un tablero compartido. El grupo luego revisa las contraseñas de los demás y les pone un puntaje del uno al cinco. Una calificación más alta corresponde a una contraseña más fuerte.

También puedes usar algunas herramientas de terceros que te ayudarán a estimar la fortaleza de las contraseñas, como esta o esta otra. Si bien son útiles para evaluar la fuerza de una contraseña, recuerda que no es más que una estimación. Finalmente, suma los puntajes de la primera ronda.

La segunda ronda introduce el razonamiento y el enfoque de los participantes para crear contraseñas seguras, y añade una tarjeta de puntuación adicional del uno al cinco, según la calidad y fiabilidad del enfoque adoptado.

Trata de lograr un equilibrio para desafiar a los niños pero sin ser demasiado competitivo. Ten cuidado con el lenguaje que utilizas para que sea veraz y respetuoso a la vez, así logras motivar a los adolescentes a poner en práctica el pensamiento crítico. Suma las puntuaciones y después ingresa las contraseñas en un administrador de contraseñas para revelar los resultados de los nuevos intentos. Recompensa a los ganadores y luego conversen sobre los enfoques tomados y lo que han aprendido.

Pide a los jóvenes que expresen sus argumentos y expliquen su estrategia en detalle. Pueden usar teléfonos inteligentes y navegar por la web para obtener algunos consejos sobre estrategias reco-

mendadas. Luego, podrían mostrarte de dónde exactamente sacaron los consejos de Internet. También podrías pedirles que te pasen algunas páginas de confianza a las que acudir para buscar recomendaciones de seguridad.

Otra opción es jugar en equipos de "parejas de padre/madre e hijo/a", aprendiendo y cerrando la brecha generacional y al mismo tiempo usando las tecnologías digitales. Cuando hables sobre la creación de contraseñas, asegúrate de hacerles a tus hijos suficientes preguntas para que reflexionen y propongan sus propias ideas.

A los adolescentes les encanta que los consideren maduros y listos. Valoran poder compartir su experiencia cuando se necesita. Si tienes más adolescentes de 13 a 18 años en la familia (hermanos, primos o incluso amigos de la familia), utiliza la variante del juego "niños que enseñan a sus padres". Juega en equipos de distintas generaciones. La mejor versión es cuando hay un intervalo de edad considerable dentro del equipo infantil, lo que permite un aprendizaje natural entre pares mientras juegan contra los adultos.

Medidas adicionales: A medida que los niños crecen, los adultos deben alentarlos a utilizar medidas de seguridad adicionales para proteger sus contraseñas. Un administrador de contraseñas almacena en forma segura una gran cantidad de códigos complicados y en algunos casos incluye la autenticación en dos fases, que verifica la identidad de la persona que introdujo la contraseña.

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

¿Estás listo para acompañarnos en este desafío?

www.digipadres.com

ENJOY SAFER TECHNOLOGY™

eset @esetla esetla ESET Latinoamérica