# Uno de cada dos españoles no cambia nunca sus contraseñas de Internet

Multimedia

**Con motivo de la celebración, hoy jueves 6 de mayo del Día Mundial de las Contraseñas, la empresa de ciberseguridad S2 Grupo ha destacado que, en un mundo hiperconectado, son un elemento esencial para mantener la privacidad y seguridad en todas las cuentas y dispositivos conectados a la red que utiliza cada usuario**

Según una encuesta realizada por S2 Grupo desde su blog Hijosdigitales.es, se ha podido saber que el 56% de los usuarios confirman no cambiar nunca sus contraseñas y las utilizan durante años. Y más del 42% aseguran utilizar la misma clave para todo.

“Hay que tener en cuenta algo en el mundo de la red. Y es que cuanto más robusta sea una contraseña, más difícil lo van a tener los ciberdelincuentes para acceder a los datos. Nadie concibe salir de casa y dejar la puerta abierta. Pues eso es lo que hace mucha gente en Internet cuando su contraseña es débil, la misma durante años o la misma en todos los perfiles”, ha declarado Miguel A. Juan, socio-director de S2 Grupo.

“Todavía se piensa muchas veces que ´cómo un ciberatacante va a ir a por mis datos´. Sin embargo, la reflexión debería ser otra: ´por qué no?´ . Ls fotos, las conversaciones, los contactos, las claves de acceso al banco, etc., valen muchísimo más de lo que a priori se puede pensar en el mercado negro de la ciberdelincuencia. Se pagan fortunas a cambio de datos”, ha asegurado José Rosell, socio-director de S2 Grupo.

El equipo de expertos de S2 Grupo ha elaborado un decálogo con 10 consejos para crear buenas contraseñas:

1. No utilizar datos familiares.- esto dejaría más expuestas a personas conocidas o a contactos de las redes sociales.
2. Evitar palabras o series de números.- Los hackers utilizan sistemas automáticos para descifrar contraseñas que hacen uso de diccionarios de palabras y generan combinaciones de números. Según estudios realizados recientemente, las peores contraseñas son ‘123456’, ‘password’, ‘abc123’, ‘qwerty’, etc.
3. Escoger contraseñas robustas.- Las claves han de tener 8 caracteres mínimo, mayúsculas, minúsculas, números y símbolos del teclado.
4. Nunca “guardar la contraseña”.- Aunque es una medida muy cómoda que el navegador recuerde la contraseña, se puede comprometer seriamente la privacidad.

5. Escoger claves memorizables pero que no sean adivinables.- Para que recordarlas no sea un problema, se puede utilizar alguna palabra o combinación de números que sea familiar y acompañarlo del resto de elemento de una contraseña robusta, por ejemplo.
6. Utilizar claves diferentes para cada servicio.- Si se utiliza un mismo código para todo y éste es descifrado por un ciberatacante, se estará comprometiendo la seguridad de todos los servicios y dispositivos de un individuo. Por este motivo, es esencial que sean diferentes.
7. Cambiar las contraseñas periódicamente.- Si se quiere incrementar la seguridad, es muy importante renovar los passwords periódicamente. De esta forma se evitará que si en algún momento otra persona pudo tener acceso a ellos, pueda utilizarlos.
8. Mantenerlas en secreto.- La mejor forma de que otras personas no puedan acceder a las cuentas es no compartirlas contraseñas con nadie.
9. Anotarlas en un lugar seguro.- Si se quiere registrarlas en algún lugar por si se olvidan, es aconsejable hacerlo en algún lugar seguro en el hogar y nunca hacerlo en el ordenador, la tablet o el smartphone.
10. Uso de aplicaciones.- Cada vez hay mayor número de apps que pueden ayudar a cifrar las claves para salvaguardarlas de una forma adecuada y poder recordarlas en caso de que sea necesario.

Hijosdigitales.es
Este blog desarrollado por S2 Grupo cuenta con más de 10.000 visitas diarias de todo el mundo y se ha consolidado como un punto de encuentro de padres e hijos para fomentar el uso seguro de la tecnología.

En él trabaja un grupo de profesionales especializados en seguridad, redes sociales y tecnología con el objetivo de ofrecer información de interés que sea de ayuda para colectivos que pueden estar desprotegidos si hacen un uso inadecuado de este tipo de dispositivos y herramientas.