DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/all/themes/mincom/logo.png

DOMPDF_ENABLE_REMOTE is set to FALSE
file:///var/www/html/portal_mincom_v2/sites/default/files/styles/noticias/public/fuente-shutterstock_autor-florida3d_contrasena-684x513.jpg

Fuente:
Silicon

Los expertos advierten de que las contraseñas cortas son peores que las largas y de que nunca se deberían reutilizar contraseñas antiguas.

Aprender a elegir contraseñas férreas es vital para evitar ataques de ciberdelincuencia que se producen por su robo o adivinación. Al menos hasta que estas contraseñas puedan ser reemplazadas en el futuro por otro método de identificación más difícil de pervertir.

¿Qué es lo que aconsejan los expertos para conseguir contraseñas realmente seguras? ¿Qué es lo que hay que hacer y lo que se debe evitar a toda costa?

ESET indica que, en primer lugar, lo que no se debe hacer es usar contraseñas compuestas únicamente por una palabra. Mejor si se recurre a frases y éstas se alteran con la adición de algunas mayúsculas, números y caracteres especiales. Con este simple cambio ya se habrá fortalecido el acceso.

En este mismo sentido, esta compañía de seguridad advierte de que las contraseñas cortas son peores que las largas.

Otros de sus consejos pasan por ir modificando las contraseña de forma periódica, nunca reutilizar contraseñas viejas, elegir una contraseña diferente para cada cuenta online y servirse de herramientas como los administradores de contraseñas o tecnología como la verificación en dos pasos.

“Desde ESET recomendamos que cada cuenta tenga su propia clave para evitar inconvenientes. En este sentido la utilización de una solución de seguridad que permita gestionar las contraseñas evita la presión de tener que recordarlas todas”, ahonda Camilo Gutierrez, jefe del Laboratorio de Investigación de ESET Latinoamérica.

Estas contraseñas “deben ser fuertes y robustas, combinando letras y números y evitando información personal obvia. En cuanto a la longitud, se recomiendan al menos doce caracteres”, sigue Gutierrez. “Es útil la creación de frases para que sean más fáciles de recordar. Por último, con el uso de un segundo factor de autenticación, se tendrá una barrera más para protegerse de los atacantes”.

Disponible en:

http://www.silicon.es/crear-contrasena-segura-2350146?inf_by=592c83d6671db80d1b8b47fd [1]

Links
[1] http://www.silicon.es/crear-contrasena-segura-2350146?inf_by=592c83d6671db80d1b8b47fd