Publicado en Madrid el 29/01/2019

10 consejos para conseguir contraseñas a prueba de hackers, según IMF Business School

IMF Business School ha realizado un decálogo con 10 consejos para conseguir una contraseña a prueba de hackers

7 de cada 10 usuarios utilizan la misma contraseña para diferentes cuentas de correo electrónico.

Se prevé que para 2022 las ofertas de trabajo en ciberseguridad se tripliquen, según datos de Cybersecurity Ventures.

IMF Business School ha realizado un decálogo con 10 consejos para conseguir una contraseña a prueba de hackers.

Hace unos días se hacía publica la noticia de que cerca de 800 millones de direcciones de correo electrónico habían sido hackeadas en una operación, denominada Collection #1 que supondría el mayor robo de datos de la historia. Sin embargo, de todas esas cuentas solo se encuentran 22 millones de contraseñas únicas. Eso significa que 7 de cada 10 usuarios repite contraseña en Internet.

Por este motivo, y coincidiendo con la celebración del Día Europeo de la Protección de Datos (28 de enero), IMF Business School ha elaborado un decálogo con 10 consejos para conseguir una contraseña a prueba de hackers que ayude a mantener los datos a salvo:

Cuánto más completa, mejor. Utilizar un mínimo de ocho caracteres y, a su vez, combinar mayúsculas y minúsculas, números o caracteres especiales para multiplicar el tiempo de hackeo.

Reutilizar está prohibido. Usar contraseñas diferentes para cada cuenta, ya sea de correo como perfiles en redes sociales o bancaria. De esta forma, si una fuera hackeada el resto continuaría a salvo.

Memoria de elefante. Nada de anotarla en un post it y dejarlo al lado del ordenador. De esta forma, ayuda a cualquiera a entrar en la cuenta y a acceder a todos los datos.

123456789. Evitar claves comunes y fáciles de descifrar como nombre, fechas de nacimiento o códigos recurrentes.

Gestores de contraseñas, los mejores aliados. Estos servicios ayudan a aquellos que tienen problemas para memorizar contraseñas o que manejan un número considerable de ellas.

Nada del documento “claves”. Muchos guardan en el escritorio un documento con todas las contraseñas, una alfombra roja para los intrusos.

Apostar por las preguntas. Esta doble barrera reduce las posibilidades de que la cuenta sea hackeada.

Adiós al “recordar clave”. Esta opción puede parecer maravillosa, pero se transforma en un error fatal si se pierde o se comparte el ordenador o dispositivo.

Periodicidad. Cambiar las contraseñas regularmente aumenta su seguridad.

¡Alerta! ¡Mirones! Ocultar siempre la contraseña mientras se introduce. Nunca se sabe quién puede estar mirando.

Estas son algunas claves para evitar los temibles hackeos que todos los datos apuntan que no dejarán de aumentar en los próximos años, al igual que los puestos destinados a ponerles freno. De hecho, se prevé que para 2022 las ofertas de trabajo en ciberseguridad se tripliquen, según cifras de Cybersecurity Ventures. Para dar respuesta a esta importante demanda, desde IMF Business School han diseñado un nuevo Máster en Ciberseguridad con modalidad online y presencial de la mano de empresas punteras en el sector como Deloitte.

Datos de contacto:
Rocio Gallego

Nota de prensa publicada en: Madrid

Categorías: Nacional E-Commerce Ciberseguridad