Prácticas que ponen en riesgo la seguridad de las cuentas digitales

La contraseña sigue siendo un método extendido para proteger el acceso a los servicios digitales, pero la popularidad de su uso no significa que los usuarios sepan cómo crear una que sea robusta, ya que muchos persisten en prácticas poco seguras como usar siempre la misma o utilizar palabras o combinaciones numéricas fáciles de adivinar.

Este jueves 4 de mayo se celebra el Día de la Contraseña, una fecha que busca concienciar sobre la importancia de este elemento de seguridad para evitar el robo de identidad, el fraude y la intrusión en cuentas personas como el correo electrónico, las de las redes sociales o las bancarias.

En este contexto, expertos como los de Kaspersky alertan de que sigue habiendo un 20 por ciento de españoles que siempre usan las mismas contraseñas para proteger sus cuentas, una práctica contraria a las recomendaciones más habituales que incluyen revisar las claves existentes y crear nuevas mucho más seguras.

Precisamente, como las recomendaciones son siempre las mismas y ya conocidas, para concienciar de la importancia de una buena contraseña, en esta ocasión se opta por el proceso contrario: las malas prácticas que hacen que la cuenta del usuario tenga mayores probabilidad de ser ‘hackeada’.

En este sentido, y siguiendo la advertencia de Kaspersky, usar la misma contraseña en todas las cuentas pone en riesgo el control de dichas cuentas y la información que hay en ellas. Esto es porque si en una brecha de seguridad se filtran las credenciales de una, el ciberdelincuente que se haga con ellas podrá acceder al resto de cuentas del usuario sin esfuerzo, con solo probar a introducir usuario y contraseña en distintos servicios.

Desde NordPass profundizan en esta mala práctica al señalar las cuentas que el usuario mantiene activas pero no utiliza, en ocasiones porque se ha olvidado de ellas. Por ello, señala la importancia de conocer el número exacto de las cuentas activas y eliminar las que estén sin uso, para «evitar lagunas en la gestión de tus contraseñas».

Otra práctica habitual es la de utilizar contraseñas débiles.

Desde NordPass apuntan que suelen ser combinaciones de números, letras y símbolos fáciles de usar en el teclado, como la típica y nada segura ‘123456’, o incluso la propia palabra ‘password’ o ‘contraseña’. Los nombres propios (Andrea, Alejandro y Cristina) también se identifican entre las claves menos seguras, al igual que las relacionadas con el deporte, como el equipo favorito de fútbol.

Por el contrario, si se opta por una contraseña larga, de al menos 10-12 caracteres, que combine números, mayúsculas, minúsculas y símbolos en secuencias no reconocibles, se estará dotando de mayor rosbustéz a esta línea de defensa de los servicios digitales.

La comodidad y las pocas ganas de pensar nuevas contraseñas y recordarlas están detrás de los principales fallos, y por ellos también es útil recurrir a un gestor de contraseñas, donde las claves se almacenan la información de forma encriptada.

Por último, hay quien establece una contraseña con la intención de no volver a cambiarla. Pero esto también supone un riesgo, aun si se trata de una clave robusta, porque en caso de robo o pérdida, los ciberdelincuentes puedan utilizarla por un periodo largo de tiempo, con la consecuencia de un mayor daño para el damnificado. Por ello, conviene revisar las contraseñas periódicamente y cambiarlas cada pocos meses.

A modo de resumen, «utilizar contraseñas diferentes para cada cuenta, así como que estas sean robustas y cambiarlas de forma frecuente es clave para mantener la seguridad de las cuentas», apunta el Senior Security Researcher de Kaspersky, Marc Rivero.

Con información de PortalTic