Las contraseñas siguen siendo el método de autenticación dominante

Aunque hace bastante tiempo que los gigantes del sector tecnológico están por la labor de quitar de en medio las contraseñas como método de identificación por sus numerosos riesgos y problemas asociados, lo cierto es que estas siguen siendo la piedra angular de los procesos de autenticación en Internet. Y lo seguirán siendo en el futuro próximo, adelanta la Alianza FIDO tras realizar una encuesta a 10.000 consumidores en el Reino Unido, Francia, Alemania, Estados Unidos, Australia, Singapur, Japón, Corea del Sur, India y China.

Según los datos del estudio, más de la mitad (51%) de los usuarios siguen iniciando sesión con sus contraseñas en servicios como cuentas bancarias en línea, mientras que el 28% ya utiliza código de acceso único de los que se envían un dispositivo móvil. Solo un 14% utiliza gestores de contraseñas y es aún menor el porcentaje de usuarios que se sirve de métodos más avanzados, como utilizar aplicaciones de generación de códigos temporales (Google o Microsoft Authenticator, por ejemplo), claves de seguridad como YubiKey y Google Titan, etc.

De acuerdo a estos datos, la mera utilización de contraseñas ha caído «un 5% para los servicios financieros, un 7% para las cuentas de trabajo, un 8% para las redes sociales y las cuentas de transmisión, y un 9% para dispositivos domésticos inteligentes» en los últimos años en favor de metodologías más eficaces y seguras. Pese a ello, las contraseñas siguen siendo el método estrella para todos los procesos de autenticación con servicios en línea, así como las causantes de muchos de los problemas de seguridad derivados de los mismos.

«Por ejemplo, el 70% de las personas tuvo que recuperar una contraseña al menos una vez en un mes determinado. Los proveedores de servicios y los minoristas también se vieron afectados, con el 59% de las personas renunciando al acceso a los servicios en línea en un mes determinado y el 43% abandonando las compras porque no podían recordar su contraseña», explica FIDO en su informe. El problemas de fondo, no obstante, es que todavía no se ha implantado una solución accesible y universal al uso tradicional de contraseñas.

Es decir, que los métodos que se suelen recomendar como

complementarios al uso de contraseñas para una doble autenticación, siguen sustentándose en la misma metodología, cuando no agregando un factor de riesgo añadido que no siempre se tiene en consideración como es qué sucede cuando se tiene acceso al medio de verificación en el que se basan casi todas esas recomendaciones. En los cimientos de todo proceso de identificación permanecen las contraseñas y hasta que se reemplace por otro igual de efectivo, las contraseñas siguen y seguirán siendo el método de autenticación dominante.

Así que, no, la identificación por huellas o caras, no está lista para ocupar el lugar de las contraseñas, mientras se siga dependiendo de un medio de apoyo que se puede extraviar con tanta facilidad como un dispositivo móvil (lo mismo para métodos avanzados como llaves físicas). Por eso, no te despistes: aplica buenas prácticas gestionando tus contraseñas, lo cual incluye sin excusas que valgan, el usar un gestor de contraseñas. Y luego, sí, todo lo demás.

Con información de Muy Computer