DIARIO de IBIZA

Publicación	Diario de Ibiza General, 33	Fecha	09/05/2023
Soporte	Prensa Escrita	País	España
Circulación	4555	V. Comunicación	4 627 EUR (5,104 USD)
Difusión	3785	Tamaño	436,82 cm² (70,1%)
Audiencia	17 732	V.Publicitario	1562 EUR (1723 USD)

Tecnología. Apple, Google y Microsoft quieren acabar con estas credenciales de acceso y han creado la Alianza FIDO, también conocida como identidad rápida en línea, que promueve un nuevo estándar común de inicio de sesión sin contraseña.

Las contraseñas se acercan a su fin

▸ La gran cantidad de servicios que requieren claves hace que sea habitual utilizar la misma para todos, lo que las hace muy vulnerables a los ataques

ÁGATHA DE SANTOS

■ Vivimos rodeados de contraseñas. Hasta tienen su Día Mundial de la Contraseña, el primer jueves de mayo. Las necesitamos para acceder a las redes sociales, al correo electrónico, a la banca electrónica, a la app del Sergas... De hecho, se calcula que la media de servicios de internet que usa cada ciudadano es de cuarenta. Y a medida que aumentan las actividades y gestiones que podemos realizar a través de internet, también aumenta el número de contraseñas, lo que hace que usar combinaciones sencillas y fáciles de recordar, y emplear la misma para todo se haya convertido en un hábito. El problema es que, de esta forma, quedan muy expuestas a posibles ataques. Esto explica la obsolescencia de las claves de acceso, que podría tener los días contados ante innovaciones más eficaces y eficientes, como los sistemas biométricos y los certificados digitales.

Según Fernando Suárez, presidente del Consejo General de Colegios Profesionales de Ingeniería Informática (CCII) y del Colexio Profesional de Enxeñaría en Informática de Galicia (CPEIG), las contraseñas podrían tener sus días contados, ya que son muy vulnerables a los ataques. «Las contraseñas se diseñaron hace varias décadas porque eran necesarias para acceder a equipos o entornos compartidos. Después, con el desarrollo de internet, se emplearon también para acceder a los distintos servicios de la nube y en todo este tiempo no se han actualizado, por lo que hoy son poco robustas y fiables por el mal uso que hacemos de ellas. Cada vez accedemos a más servicios que las requieren y lo habitual es utilizar el mismo usuario y contraseña, que es fácil de recordar y, por tanto, fácil de vulnerar», explica.

Nadie puede augurar cuándo será sustituido el sistema de contraseñas, pero lo cierto es que su final parece estar cada vez más cerca. Ya hay otros sistemas más seguros y efectivos, como la biometría, y, lo que es más importante si cabe: las grandes compañías tecnológicas –Apple, Google y Microsoft– también quieren acabar con estas credenciales de acceso y han creado la Alianza FIDO, también conocida como identidad rápida en línea, que promueve un nuevo estándar común de inicio de sesión sin contraseña.

«Las contraseñas tienen fecha de caducidad. Hay sistemas mucho más seguros, como la biometría y los sistemas de certificado digital. El problema de estos sistemas es que suponen un pequeño esfuerzo adicional por parte del usuario que muchos no están dispuestos a hacer porque aún no somos conscientes del riesgo de usar contraseñar débiles ni de las implicaciones que tiene una vulnerabilidad de seguridad en internet. Aún no percibimos el valor de nuestros datos en internet», comenta.

Una contraseña débil puede dar lugar a ciberataques con la intención de usurpar la identidad, secuestrar datos o robar, entre otros ciberdelitos. Este daño puede verse multiplicado si la contraseña *hackeada* es la puerta de entrada a todos los servicios del usuario.

Inteligencia artificial

La tecnología biométrica, basada en la inteligencia artificial (IA), es una de las alternativas más prometedoras, ya que es una manera sencilla, rápida y segura de acreditarse para acceder a un servicio digital. Se basa en el concepto *lo que soy*, frente a los de *lo que sé* y *lo que tengo* en los que se fundamentan las contraseñas clásicas. Es un sistema sobradamente extendido, ya que lo incorporan los dispositivos móviles de última generación, a los que se accede a través del reconocimiento del iris, la imagen facial o la lectura de la huella digital del usuario.

«Las contraseñas tienen ya fecha de caducidad. Hay sistemas más seguros», sostienen los expertos

Suárez explica que la biometría es uno de los requisitos que incorporan los denominados sistemas de doble autentificación, es decir, sistemas que piden, además de la contraseña del usuario, un segundo requisito, que puede ser la huella dactilar, la confirmación por email para completar una actividad o introducir un número o una clave enviada por el proveedor, de modo que, aunque la contraseña sea robada no sea suficiente para acceder al servicio. Según el informático, el problema de este sistema es que no depende tanto del usuario como de que el proveedor permita utilizar esta doble identificación.

Otra alternativa es el certificado electrónico, que funcionaría como un DNI electrónico. «El DNI en España tiene un certificado de firma y otro de autenticación, por lo que es muy difícil de vulnerar. Sin embargo, también es cierto que su uso no es tal sencillo porque se necesita un lector de tarjetas», comenta.

Sencillos y gratuitos

Existen también sistemas, sencillos y gratuitos, que pueden hacer menos vulnerables los servicios protegidos con clave, como gestores de contraseñas como LastPass y One Paswood, que, aunque siguen utilizando el modelo de usuario y contraseña, no obligan al usuario a recordarlos, sino que es el propio programa el que los recuerda. Estos sistemas pueden, además, generar contraseñas individuales para cada servicio, robustas y difíciles de memorizar y, por tanto, que no sean vulnerables a un *ataque de diccionario* –técnica que consiste en probar muchas palabras recogidas en los diccionarios y también las contraseñas más usadas como 1,2,3,4,5,6– para tratar de romper las barreras de acceso. Aunque la inteligencia artificial (IA) no es el mayor riesgo para las contraseñas, Suárez reconoce que supone otro reto. «La IA lo que hace es aprovecharse de acceder a muchísimos datos y si nuestra clave es nuestra fecha de nacimiento, por ejemplo, con la IA se podría acceder de forma sencilla» asegura.

En el caso de que el usuario decida crear sus propias contraseñas al modo tradicional, Suárez recomienda que ésta sea robusta, es decir, que contenga letras, números y símbolos; que cree una diferente para cada servicio; que no estén basadas ni en fechas señaladas, como cumpleaños ni nombres de hijos o de mascotas; y que se cambien de vez en cuando. También recomienda que no las comparta con nadie. Las contraseñas para acceder a los distintos servicios de internet son personales y por seguridad nadie debe de tener acceso a ellas.