¿Los usuarios están preparados para un mundo sin contraseñas digitales?

El fin de las contraseñas digitales, un sistema de conexión considerado poco fiable por expertos y grandes tecnológicas, **choca con la dificultad de los usuarios para adaptarse a nuevos sistemas**.

“La era de las contraseñas está llegando a su fin”, escribieron en diciembre en su blog dos responsables de Microsoft. Al igual que el resto de grandes tecnológicas, ellos promueven sistemas más seguros. Entre ellos, las huellas dactilares, el reconocimiento facial o el sistema de las llamadas “llaves de acceso”.

El gigante estadounidense quiere soluciones “más seguras” y lleva años preparándose.

Desde mayo, las cuentas de nuevos usuarios funcionan por defecto con sistemas de conexión más sofisticados que las contraseñas tradicionales.

En Francia, la agencia tributaria reforzó su política de seguridad informática.. De esta manera, obliga a los usuarios a validar su conexión con un código que reciben por correo electrónico, además de la contraseña.

“Las contraseñas suelen ser débiles y reutilizadas”, explica a AFP Benoît Grünemwald, experto en ciberseguridad de la compañía Eset. Asimismo, **recuerda que los hackers pueden descifrar en minutos o incluso en segundos** aquellas que tienen menos de ocho caracteres.

Además son un objetivo frecuente de las filtraciones de datos. «Cuando están mal almacenadas por quienes se supone que deben protegerlas y guardarlas», apunta Grünemwald, algo puede salir mal.

En junio, investigadores del medio Cybernews descubrieron una gigantesca base de datos con 16.000 millones de nombres de usuario y contraseñas procedentes de archivos pirateados, una prueba más de la magnitud del problema.

¿De contraseñas a…?

La asociación industrial **Fast Identity Online Alliance (FIDO)**, que cuenta entre sus miembros a Google, Microsoft, Apple, Amazon y TikTok, trabaja para fomentar la adopción de conexiones sin contraseña y promueve el uso las conocidas como “llaves de acceso”.

Este sistema utiliza un dispositivo externo, como un teléfono, para autorizar las conexiones mediante un código PIN o una conexión biométrica (huella dactilar o reconocimiento facial), en lugar de la contraseña.

Una manera de proteger a los internautas, subraya Troy Hunt, responsable del sitio Haveibeenpwned (“¿He sido víctima?”, en inglés), porque “con las llaves de acceso, no puedes dar accidentalmente tu llave a un sitio malicioso”.

Sin embargo para el experto australiano esto no significa el fin de las contraseñas.

“Hace 10 años (…) la gente decía ‘¿Seguiremos teniendo contraseñas dentro de 10 años?’, y la realidad es que tenemos más contraseñas que nunca”, destaca.

Aunque las grandes plataformas refuerzan la seguridad de las conexiones, muchas webs siguen funcionando con contraseñas simples. Y para los usuarios, la transición no es fácil.

Las llaves de acceso requieren instalar un sistema específico y si se olvida la contraseña o se pierde el teléfono registrado como “dispositivo de confianza”, es más difícil recuperarla.

“La ventaja de las contraseñas, y la razón por la que las seguimos usando, es que todo el mundo sabe cómo utilizarlas”, subraya Hunt.

Con información de El Nacional