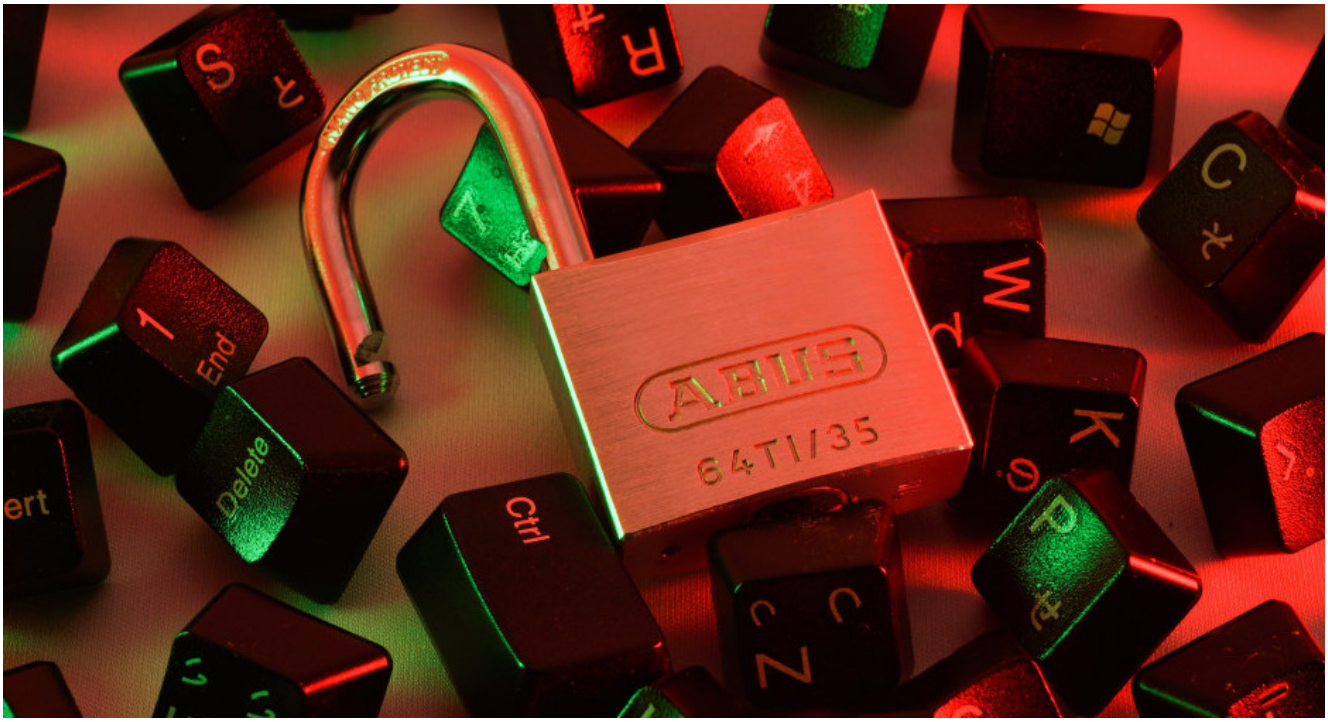
Contraseñas en extinción: ¿por qué en algún momento dejarán de existir y cómo se reemplazarán?

20/08/2023



Hoy en día es bastante sencillo para los ciberdelincuentes descifrar contraseñas en minutos. Esto se debe al avance de la tecnología, principalmente a las técnicas de ingeniería social en combinación con inteligencia artificial. Debido a esto, los expertos recomiendan que los usuarios actualicen sus claves cada tres meses.

Ahora bien, muchas veces las personas le dan más prioridad a la comodidad que la seguridad, eso es lo que explica que el 35% de los usuarios latinoamericanos usa siempre las mismas contraseñas. Igualmente, este sistema de acceso se está volviendo cada vez menos frecuentes ya que aparecen otros métodos de autenticación que son más cómodos y seguros.

En muchas ocasiones, los usuarios son responsables de este

fenómeno o dicho de otra manera, le facilitan a los ciberdelincuentes hacer su trabajo con mucha más facilidad. Como explica Martina López, investigadora de seguridad informática de ESET Latinoamérica, “la reutilización de credenciales también ha contribuido a la vulnerabilidad de las contraseñas escritas. Los usuarios tienden a utilizar las mismas contraseñas para múltiples servicios debido a la dificultad de recordar y administrar varias contraseñas únicas. Entonces, cuando un atacante obtiene acceso a una cuenta con credenciales reutilizadas, es probable que también pueda acceder a otras cuentas del mismo usuario, lo que aumenta el daño potencial y la cantidad de datos comprometidos”, afirma.

La responsabilidad de las empresas

Aunque hay empresas que están empezando a exigirle a los usuarios diferentes requisitos al momento de crear una contraseña, el problema va más allá y muchas veces esas mismas empresas no siguen ciertos requerimientos importantes: “Por ejemplo, si yo tengo una tienda en línea, **un criminal puede invadir mi sitio web y obtener la base de datos con los mails de los clientes**. Es decir que el problema está en cómo las empresas y las entidades cuidan nuestras contraseñas”, explica **Fabio Assolini, director del Equipo de Investigación y Análisis Global para América Latina en Kaspersky.**

A su vez, existe la compraventa de bases de datos de credenciales robadas y mismo los delincuentes luego apuntan a múltiples sitios para obtener acceso, sabiendo que algunos usuarios reutilizan las contraseñas. De esta forma, el Foro Económico Mundial sostiene: “en términos de ciberseguridad, **la gestión de contraseñas débiles es fundamental para todo el ecosistema criminal”.**

Hoy los delincuentes pueden descifrar contraseñas en minutos mediante técnicas de ingeniería social en combinación

con inteligencia artificial. Foto Unsplash.

En esta línea, López explica que últimamente los métodos de autenticación que no tienen que ver con contraseñas escritas han ganado popularidad y se utilizan cada vez más porque “las brechas de seguridad y filtraciones masivas de contraseñas a lo largo de los años han puesto de manifiesto la **fragilidad de depender únicamente de las contraseñas escritas”.**

Otras formas de autenticación

Amazon, Google y Microsoft son algunas de las firmas que apoyan la eliminación de contraseñas. Por ejemplo, Google Workspace tiene un programa experimental para habilitar claves de acceso como reemplazo de las contraseñas. De esta manera, el nuevo método de inicio de sesión brinda a los usuarios empresariales un **medio de autenticación a través de huellas dactilares y reconocimiento facial, entre otros.**

Afortunadamente, las contraseñas no son la única forma de autenticación. Por ejemplo, la **autenticación de múltiple factor** (MFA, por sus siglas en inglés) es la práctica de usar más de un método para verificar que los usuarios son quienes dicen ser. “Por ejemplo, un sistema banca online puede requerir que los clientes ingresen su nombre de usuario y contraseña, y luego **un código que se envía a su teléfono móvil por mensaje de texto”**, ilustra **Martín Medina, BDM de ciberseguridad en BGH Tech Partner.**

Dentro de las alternativas está el **acceso por biometría**, que se basa en los atributos físicos que identifican de forma única a las personas. Como siempre los tenemos con nosotros, son fáciles de usar. Estamos hablando de **huellas dactilares, reconocimiento facial y de iris**. Sobre este tema, desde la firma Veritran aclaran que la biometría se perfila como una **tecnología prácticamente infalible en lo que a seguridad de operaciones se refiere**, especialmente en el terreno de la banca digital. “

Otra opción es la **verificación por correo electrónico o mensaje de texto** (SMS) se llama OTP (por One-Time Password) y son códigos que se usan como una medida más para verificar la identidad de la persona que está queriendo acceder, por ejemplo, a una cuenta en una red social. **Javier Wullich, gerente de desarrollo de negocios de Plusmo, un integrador de telefonía celular que ofrece envíos masivos de SMS y servicios de mensajería omnichannel,** comenta que "el proceso de verificación vía SMS implica que el usuario registre previamente su número de teléfono móvil en una página web o aplicación, para luego poder recibir un mensaje de texto con un código de verificación que debe ingresar en la página o aplicación a utilizar". Como todos los celulares aceptan SMS sin necesidad de tener que instalar una app, se trata de una herramienta lista para usar. Además, Wullich menciona que se trata de un **medio "efectivo, rápido y fácil de usar".**

Por otra parte, está la opción llamada **Notificaciones Push**, que ocurre cuando un usuario solicita ingresar a un sitio, y para eso recibe un enlace por mensaje de texto o correo electrónico y debe activarlo para obtener acceso. Por lo general, este link caduca después de ser usado o transcurrido cierto período de tiempo.

Las claves de seguridad de hardware son otra alternativa. En este caso se conectan a dispositivos de hardware mediante tecnología USB, USB-A, USB-C, NFC y Bluetooth. Como son pequeñas, se pueden cargar en el llavero.

Recomendaciones

Dentro de los consejos que dan los especialistas, afirman que **las claves nunca deben anotarse en papeles físicos ni en archivos digitales**. Y como alternativa, recomiendan el **uso de administradores de contraseñas**. Se trata de un software diseñado para crear, administrar y proteger sus contraseñas de

manera segura. Así y todo, los administradores de contraseñas más populares han exhibido **vulnerabilidades que le permitieron a los delincuentes obtener credenciales.**

“Es poco probable que las contraseñas escritas desaparezcan por completo en un futuro cercano, ya que han sido ampliamente utilizadas y arraigadas en la seguridad informática durante mucho tiempo. Sin embargo, es posible que sigamos viendo una tendencia hacia la **adopción de otras opciones de autenticación más seguras y convenientes que complementen o mejoren la seguridad de las primeras**”, concluye la experta de ESET.

Fuente: Canal 26