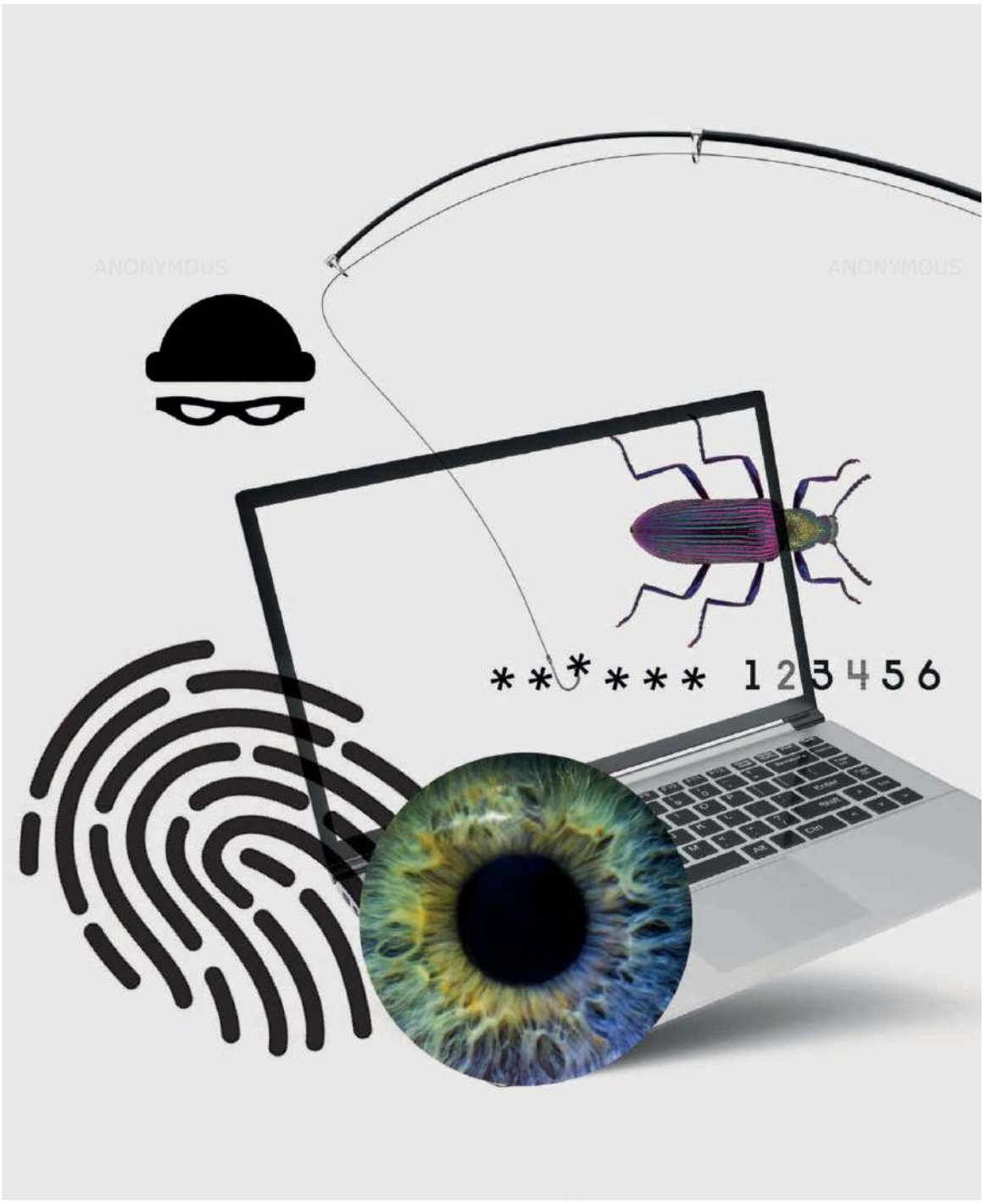
Benditas claves. Son las llaves para acceder a los servicios esenciales del mundo virtual, pero resultan demasiadas y hay que cambiarlas con mucha frecuencia. Usuarios que perdieron todo al olvidar un password cuentan sus experiencias. Y especialistas analizan si los opciones biométricas pueden ser una solución.

POR TOMÁS BALMACEDA

EL DILEMA DE CADA DÍA: ¿Y SI ME OLVIDO LA CONTRASEÑA?



Una veintena de letras y números le quitaron la alegría a Cristian, un ingeniero informático cordobés que prefiere que no se conozca su apellido "porque ya bastante sufro en soledad, no necesito que nadie me hable del tema". Hace poco más de diez años recibió algunos bitcoins como parte de pago por la migración de unos servidores y los guardó en su billetera virtual. Durante mucho tiempo no le prestó mayor atención a ese ahorro hasta que un colega le recordó el pago y Cristian intentó saber cuánto dinero tenía. Pero no pudo: había olvidado el usuario y la contraseña que había puesto años atrás. Para colmo de males, el mail que utilizaba por ese entonces ya no existía más porque habían borrado el sitio y el servidor que lo alojaba... No tenía cómo ni a quién reclamarle más que a su propio descuido.

"Pasé muchas noches sin dormir con la mente puesta en la plata que está guardada ahí sin que yo pueda usarla. Pienso en todo lo que podría ayudar a mi familia en este momento o cómo podría servirme si tengo un accidente y ya no puedo trabajar más. Trato de evitar las noticias sobre el aumento del precio del bitcoin para no amargarme, pero el año pasado escuché una conversación en un asado y calculé que perdí entre ciento veinte y ciento cincuenta mil dólares. Obvio, volví a caer en una depresión", admite Cristian.

No es el único que ha sufrido un dolor de cabeza de este tipo por culpa de los benditos passwords. El desarrollador de software estadounidense Stefan Thomas compró en 2011 cerca de siete mil bitcoins. Los alojó en un USB con contraseña, pero cuando los quiso recuperar descubrió que la había olvidado. El sistema le permite diez intentos para entrar antes de bloquearse para siempre. Ya probó ocho y decidió rendirse. Al momento de escribir esta nota la fortuna atrapada superaba los 220 millones de dólares.

Se calcula que el 20% de los bitcoins están en billeteras a las que sus dueños no tienen acceso por olvidos.

Ábrete Sésamo

En este mundo altamente digitalizado, las contraseñas son la manera en la que accedemos no sólo a nuestras billeteras virtuales sino también a nuestras cuentas de banco, cajeros automáticos, correos electrónicos, redes sociales, computadoras de trabajo y un sinfín de servicios esenciales. No se trata de un fenómeno nuevo: las contraseñas existen desde tiempos inmemoriales y siempre han sido problemáticas.

En la leyenda de *Alí Babá y los cuarenta ladrones*, el protagonista escucha sin querer la frase secreta que utiliza una banda de ladrones para ingresar a una cueva en la que encuentra un tesoro fabuloso, pero de la que roba una sola bolsa de monedas para no despertar sospechas.

Cuando le cuenta la historia a su hermano, éste decide ir a la cueva para llevarse un botín mucho más grande, pero su codicia lo delata y lo asesinan brutalmente. Alí Babá consigue vengar su muerte y asesina a los ladrones, volviéndose el único poseedor de la clave a la cueva.

Mientras que para Cristian la contraseña para acceder a su fortuna en bitcoins es una serie de letras y números que no consigue recordar, para el héroe de *Las mil y una noches* era decir simplemente "Ábrete Sésamo". Ya sea una billetera cripto o una cueva mágica, todo depende de conocer la contraseña.

En *Una historia de las c0ntr4s3ñ4s*, libro que llegará en abril a la Argentina a través de Ediciones Godot, el profesor de literatura y tecnología inglés Martin Paul Eve explica que usar una contraseña involucra presentar un desafío y recibir una respuesta.

Quien desea confirmar la identidad de otra persona pedirá la contraseña y la otra parte debe brindar un conocimiento previamente compartido y acordado para demostrar su identidad.

En esencia, responder correctamente el desafío implica verificar que una persona conoce una palabra o frase específicas. Si se cree que un individuo y solo ese individuo puede saber esa clave, entonces se asume que ese conocimiento identifica a dicha persona. Sin embargo, no sólo es posible que nos olvidemos la palabra justa, como le pasó a Cristian, sino que alguien más podría conseguirla, como sucedió con Alí Babá.

"Podemos ver a una contraseña como

ENTRE LA FALTA DE MEMORIA Y EL HARTAZGO

-

Según un estudio de News Wire, una persona debe recordar en promedio entre 70 y 80 contraseñas a lo largo de su vida. Los consejos son que los usuarios elaboren claves complejas y únicas, que las recuerden y cambien con frecuencia pero pocas personas lo hacen.
En una encuesta reciente elaborada por Microsoft, una de cada cinco personas afirmó que prefería "responder a todos por error un correo electrónico" que cambiar su contraseña. Al mismo tiempo, casi un tercio de las personas prefieren dejar de utilizar por completo una cuenta o un servicio que lidiar con una contraseña olvidada.

LA HUELLA DIGITAL
Una opción que no requiere de la memoria y es personalísima. Pero los expertos alertan: se podría utilizar con el usuario inconsciente. Es decir, no es 100% segura.

una llave: hay puertas que no necesitan llaves, porque no es necesario proteger lo que tiene dentro, como cuando entramos a una página web o a una plaza; pero sí cerramos con llave la puerta de nuestra casa o de la oficina. Lo mismo pasa con nuestras redes sociales o nuestra cuenta bancaria, por ejemplo. La plataforma necesita saber que somos nosotros los que queremos acceder y no otra persona. Las contraseñas son esa manera de validar la identidad del usuario", le explicó a *Viva* Martina López, investigadora de Seguridad Informática de ESET Latinoamérica.

Marcela Pallero, directora del Programa Seguridad en TIC de la Fundación Sadosky, le suma un elemento más a la metáfora: "Además de la llave hay que tener en cuenta la cerradura. E, incluso, cómo está construida la puerta y toda la casa, porque tal vez eso que estamos cuidando es accesible por otros medios. Los sistemas que usan contraseñas dependen, por un lado, de la cadena de caracteres y, por otro, de la plataforma o sistema que las valida y almacena. Por ejemplo, la cantidad mínima de caracteres que admiten y los tipos de caracteres, la cantidad de veces que te podés equivocar antes de que el sistema se bloquee e impida seguir haciendo pruebas".

SE CALCULA QUE EL 20% DE LOS BITCOINS ESTÁN EN BILLETERAS VIRTUALES A LAS QUE SUS DUEÑOS NO TIENEN ACCESO POR OLVIDO DE LA CONTRASEÑA.

...

"Hay formas de adivinar ese conjunto de caracteres –agrega Pallero–, generalmente basadas en técnicas de ingeniería social, que son las que se utilizan para conseguir información de distintas fuentes como redes sociales, fuentes públicas o engaños clásicos. Alguien puede hacerse pasar por personal de salud mediante un llamado telefónico y preguntarnos cuántas vacunas o qué enfermedades tuvimos y obtener información confidencial, por ejemplo."

Así, estas "llaves" son muy problemáticas y se están volviendo un creciente dolor de cabeza para todas las personas: parece que no podemos escapar de ellas y cada vez necesitan ser más complejas, deben ser renovadas periódicamente y

no es una buena idea usar la misma para todos los servicios. Pero la gran pregunta es: ¿quién puede recordarlas todas sin equivocarse?

Malditopassword

Perder una contraseña también puede tener consecuencias sentimentales fuertes: Enzo, por ejemplo, es un porteño de 42 años que había digitalizado fotos de su infancia y juventud para guardarlas en una cuenta de Yahoo! Cuando su padre falleció durante la pandemia, quiso volver a ver esas fotos y descubrió que hacía casi una década que no entraba a esa casilla de correo y que no recordaba la contraseña.

"Ahí hay fotos que no sé si volveré a recuperar y el sistema sólo me deja hacer tres intentos antes de bloquearme por 24 horas. Ya probé las combinaciones que me parecían razonables pero ninguna funciona. Hasta llamé a mi ex novia a ver si ella recordaba qué contraseña usaba por entonces... Por supuesto que no tenía idea", reveló.

De todos modos no pierde las esperanzas: cree que debe haber escrito la clave en algún cuaderno o dentro de algún libro y espera alguna vez encontrarlo. Sólo debe confiar en que para ese entonces su cuenta siga activa y los servidores de Yahoo! sigan funcionando.

"En el fondo, es el mismo problema que tenemos hoy con los números de teléfono: yo recuerdo perfectamente el de mi casa donde viví con mis padres, pero no sé de memoria el celular de mi mujer. Entonces, ¿cómo pretender que recordemos de memoria decenas de contraseñas? Esto nos lleva a pensar fórmulas fáciles de memorizar, como la calle donde vivimos o la fecha de nacimiento de nuestros hijos, lo que facilita a un tercero a que la adivine", plantea Santiago Cavanna, Chief Information Security Officer de Microsoft Argentina.

"Para colmo de males –agrega este especialista–, a lo largo de los años se fueron acumulando bibliotecas de contraseñas que se obtuvieron después de filtraciones o ciberataques. Entonces hoy podés comprar millones de contraseñas reales, creadas con reglas mnemotécnicas, y crear un programa que las vaya probando una a una. Esto se lo conoce como ataque de fuerza bruta y son cada vez más frecuentes."

LA GRAN DUDA DE ESTOS TIEMPOS: ¿FUIMOS HACKEADOS?

-

Es frecuente que usemos la misma contraseña en distintas plataformas, lo que hace que si alguna es vulnerada, quedemos expuestos en varios sitios. Para comprobar si tus datos han sido filtrados hay que entrar a haveibeenpwned.com, un portal que recopila las bases de datos que se filtran en la red y que tiene más de 12 mil millones de cuentas filtradas.

NADA ES GARANTÍA, PERO EL DOBLE FACTOR AYUDA

-

Aunque todos los especialistas consultados coincidieron en que no existen las contraseñas inviolables, una buena medida para implementar es sumar un segundo factor de autenticación en nuestras plataformas. Se trata de una capa extra de seguridad con un código único que llega por SMS o mediante un token por una app. "De este modo podemos disminuir sensiblemente la frontera de ataque de un delincuente", aseguró Santiago Cavanna de Microsoft.

FACE ID

El reconocimiento facial es falible. No siempre reconoce al usuario y también da falsos positivos.

Los problemas de las soluciones

Microsoft emprendió, hace tiempo, un plan para eliminar las contraseñas tradicionales que se conforman con letras, números y signos. Gracias a las aplicaciones Microsoft Authenticator y Windows Hello, cada vez que un usuario quiere ingresar a una cuenta se le envía una clave de seguridad o código de verificación a un teléfono o correo electrónico, el cual podrá utilizarse para iniciar sesión en las distintas aplicaciones, o utilizando reconocimiento facial, huella digital o un PIN.

Sin embargo, el creciente uso de información de nuestro cuerpo para validar nuestra identidad (incluso el reconocimiento del iris) despierta alarmas entre especialistas y activistas. Para Pallero, se trata de datos muy sensibles con un destino que no es claro: "Nuestros datos biométricos son muy valiosos en varios campos y pueden ser fácilmente convertidos en mercancía o parte de campañas que impactan en nuestra salud, la libertad de expresión o el targeting político".

La especialista de la Fundación Sadosky asegura que "la información biométrica es demasiado sensible como para ser simplemente utilizada en la autenticación cuando hay otros métodos. Vivimos en un momento en el que la transversalidad de la tecnología en la sociedad es total, pero seguimos pensando en estructuras muy rígidas, compartimentadas".

Tobías Schleider –filósofo, abogado y consultor en seguridad– ironiza: "La idea de usar datos biométricos para acceder a nuestros dispositivos, principalmente teléfonos celulares y computadoras portátiles, parece una buena por práctica y cómoda, pero gracias a la pizza congelada, las sandalias de plástico y algunas novelas de verano sabemos que la comodidad no siempre es la mejor opción ni la más segura".

De acuerdo con su visión, además de los problemas de almacenamiento y uso, estos procedimientos son costosos y distan de ser perfectos.

"Los falsos positivos son bastante frecuentes en estas aplicaciones, así como también los falsos negativos, lo que le concedería acceso a quien no es la persona indicada para ingresar –alerta Pallero–. Nuestro cuerpo externo es naturalmente más accesible que nuestra

memoria y bien se podría usar nuestra huella digital con nosotros inconscientes o nuestro rostro sin nuestro consentimiento. Además, no tenemos ningún control acerca de dónde van nuestros datos y para qué se usan."

¿Y si las jubilamos?

Para Cristian Borghello, especialista en Educación y Seguridad de la Información, las contraseñas tradicionales fueron pensadas décadas atrás, cuando las usaban menos personas y en menos dispositivos. Para él no sería una mala idea jubilarlas, pero el problema es que las alternativas disponibles tienen también sus propios problemas, empezando porque a los seres humanos nos cuesta cambiar de hábitos.

"Usar un gestor de contraseñas que utilice sólo una clave maestra me trae los problemas del olvido o de su fortaleza –explica–. Si la anoto en una libretita, un papel o una planilla de Excel, automáticamente se vuelve vulnerable. Si un día pierdo esa contraseña, quedo literalmente afuera de todo. Y si alguien vulnera la nube en donde se almacenan, puede acceder a toda mi información. Y aunque en un modelo de seguridad realista, la biometría es más fuerte que las contraseñas, si nos roban nuestra huella o consiguen replicar nuestro rostro estamos en problemas porque... ¡nuestra cara no puede ser reemplazada por otra! Y los criminales siempre están un paso más adelante."

LOS DATOS BIOMÉTRICOS NO SON LA SOLUCIÓN PERFECTA, YA QUE PUEDEN DAR FALSOS POSITIVOS Y FALSOS NEGATIVOS.

...

Pero no es necesario imaginar un escenario distópico en donde perdemos nuestra cara. A fines del año pasado, Julio, el dueño de una marca de ropa y accesorios para disidencias con local en la mítica Galería Bond Street, decidió intervenir su rostro y se tatuó los globos oculares de negro, un tipo de operación cada vez más frecuente. Cuando quiso acceder al dinero de su emprendimiento mediante la app de la plataforma Mercado Pago, descubrió que no le reconocía el rostro.

Probó de múltiples maneras –con lentes, sin ellos, con otra luz, incluso pegándose unos dibujos de sus ojos hechos en papel–, pero sin éxito. Tuvo que solicitar ayuda a la empresa, que le comunicó que ya no podría usar ese tipo de autenticación porque el sistema no reconocía más su cara. Desde entonces quedó afuera de uno de los métodos de autenticación de moda.

Existe, además, todo un negocio delictivo alrededor de las contraseñas. En su libro *Engaños digitales, víctimas reales*, el periodista Sebastián Davidovsky cuenta la historia de un estudio contable argentino al que le robaron, entre otras, las contraseñas de acceso a sus servidores de correo electrónico y la clave fiscal del portal de la AFIP. Así, modificaron las cargas sociales de los empleados y enviaron emails a clientes y colegas con información falsa. Consultado por *Viva*, Davidovsky cree que en el último tiempo creció la conciencia sobre la importancia de interesarse por la seguridad en

A UN ESTUDIO CONTABLE LE ROBARON LA CLAVE DE ACCESO A LA AFIP. ASÍ, MODIFICARON LAS CARGAS SOCIALES DE SUS EMPLEADOS.

...

plataformas digitales: "Me parece que es un fenómeno muy relacionado con la experiencia, ya sea la propia o la de conocidos. Los delitos informáticos van en aumento y con ellos creció la necesidad de saber más y cuidarse más".

"Nunca vamos a tener seguridad total en el ámbito digital por dos motivos: ningún sistema es completamente seguro y nosotros como usuarios siempre seremos vulnerables a engaños para obtener esa información. Creo que así como aprendimos que debemos tener medidas de seguridad distintas en la calle que en nuestra casa, como no poner el celular en un lugar muy visible o andar con la mochila abierta, terminaremos haciendo lo mismo en ámbitos digitales", puntualizó Davidovsky.

Al fin de cuentas, las cosas no cambiaron tanto entre la picardía Alí Babá al insomnio de Cristian. En palabras de Cristian Borghello: "Yo sueño con la muerte de las contraseñas, pero no lo veo como algo que vaya a ocurrir pronto". ■