ILUSTRACIÓN: SHUTTERSTOCK

Las contraseñas de cada día

Para el e-mail, las redes sociales, el banco *online*... Cómo construir claves seguras y posibles de recordar. *¿123456*? Hay mejores opciones

POR **MARTINA RUA**

Para la clave de Facebook, el nombre del hijo; para Twitter, la misma más el número uno; para la cuenta bancaria, el mismo nombre más el apellido con dos letras en mayúscula, y para el e-mail del trabajo, todo lo anterior, con dos símbolos al final. ¿El resultado? Todas las contraseñas mezcladas en la cabeza y la necesidad de resetear los claves casi a diario.

Los más de 20 millones de argentinos que utilizamos Internet a diario manejamos en promedio diez contraseñas por usuario, entre los servicios de uso personal y laboral. La mayoría, para poder recordarlas, recurre a las mismas (y obvias) fórmulas para muchos servicios, lo que deja a la información muy vulnerable a posibles hackeos o software malicioso. De hecho, el masivo hackeo de 38 millones de cuentas que se hizo a usuarios de Adobe este año demostró que casi dos millones de usuarios utilizaban *123456* como contraseña y la segunda más usada era *123456789*.

Para Armando Carratalá, gerente de IT de Certisur, muchos usuarios usan una misma contraseña para servicios que precisan alta seguridad, como el homebanking, y otros de media o baja importancia, como Facebook. "Es importante definir niveles de contraseñas para cosas de poca seguridad, como blogs o diarios, para seguridad media (correo personal o Facebook) y para seguridad alta (banco y tarjetas de crédito), y no mezclar entre ellas", recomienda.

También hay muchos trucos y reglas mnemotécnicas

para armar contraseñas fuertes. Los especialistas convergen en algunos consejos básicos: que las claves siempre contengan una combinación de números, letras y símbolos; elegir algunas letras para poner en mayúscula, como por ejemplo, aquellas que están entre la M y la Z, u otra regla similar. Para los que se animan a algo un poco más complejo se pueden armar claves que estén compuestas por una cadena de caracteres especiales con números, letras y símbolos. "Por ejemplo, con la frase *Compro una bicicleta con cinco años de uso*, la clave podría ser *C1bc5adu*", ejemplifica Gerardo Loureiro, director de Prevención de Fraude de Mercado Libre.

"También se pueden cambiar vocales por números, por ejemplo, la letra *e* por un *3*, agregar algún signo de puntuación en un lugar fácil de recordar, como en el final. Básicamente, las contraseñas deben estar ligadas a palabras, signos y números que puedan recordarse, pero ser, por su diseño y estructura, difíciles de descifrar para un tercero", define Carlos Aramburu, gerente de consumo de McAffe.

Casi 13 millones de argentinos ya utilizan Internet para operaciones bancarias, según una encuesta de Certisur y D'Alessio, y este número está en constante crecimiento. De ellos, el 47% paga servicios y el 44% efectúa compra y venta de bienes. Estos datos muestran la importancia de la seguridad en la información personal que viaja por la Web. Los accesos de máxima seguridad requieren cada vez más datos. Además del nombre de usuario y la clave, muchos bancos piden ahora un segundo paso, que es una identificación que puede variar entre una tarjeta de coordenadas –cuyos datos se cargan en el momento de transferir–, un *token* –por ejemplo el celular, que recibe una clave para autorizar la operación– o una segunda clave alfanumérica.

Damián Kalnins, especialista en seguridad de Softline Argentina, aporta los *no* rotundos a la hora de crear claves seguras: "No usar palabras que se encuentren en el diccionario ni patrones de teclado, como *qwerty*, números en secuencia (*1234*) o repetidos (*1111*)", advierte. Según Kalnins no se debe incluir nunca una contraseña en programas de mensajería, correo electrónico, ni otros dominios Web, además de no utilizar datos personales o que refieran a la vida cotidiana del usuario que son fácilmente descifrables.

Lograr contraseñas seguras no es complicado, lo difícil es recordar tanta información de tantos servicios distintos. "Una solución efectiva y que pocos usuarios usan son los gestores de contraseñas. Se trata de aplicaciones, en muchos casos gratuitas; allí se guardan encriptadas todas las claves. Así, recordando sólo una contraseña maestra, el resto está bien guardado", explica Jerónimo Basaldúa, CEO de Base4 Security y organizador de EKO Party, uno de los principales eventos de seguridad que se celebra anualmente en Buenos Aires. Algunas de las aplicaciones más populares son KeepassPasswordSafe, EfficientPassword Manager, KasperskyPassword Manager y ClavesPC. Esto evita los eternos papelitos pegados al monitor o guardados en la billetera que son una opción demasiado vulnerable. Por ejemplo la empresa McAfee ya ofrece servicios de *bóveda online de contraseñas* a los que se accede a través de rasgos biométricos como reconocimiento de voz o facial.

Existe, además, la opción de agregar una capa adicional de seguridad que se llama *Verificación de dos pasos* que la mayoría de las empresas con servicios en nubes ya ofrecen. "A las personas que opten por esta verificación, se les solicita un segundo código, vinculado a un dispositivo móvil: es un número de seis dígitos que se envía por SMS. De este modo, para que un hacker pudiera actuar debería tener acceso a estas dos informaciones", describe Martín Waserman, gerente de Políticas Públicas y Asuntos Gubernamentales para Cono Sur en Google.

Según él, también es muy importante utilizar una contraseña distinta para cada servicio y configurar las opciones de recuperación de contraseña y mantenerlas actualizadas. Entre sistemas de seguridad online, trucos y reglas, ya no quedan excusas para no darle mayor seguridad a la creciente información que volcamos a diario en el mundo digital. ●

revista@lanacion.com.ar

Consejos para el *password*

► **DEFINIR** niveles de seguridad según la información que protegen las contraseñas, desde blogs hasta cuentas bancarias, y no mezclarlas entre ellas.

► **PROCURAR** combinar números, letras, símbolos, letras mayúsculas y minúsculas.

► **CAMBIAR** vocales por números, por ejemplo, la letra *e* por un *3* y agregar algún signo de puntuación en un lugar fácil de recordar.

► **NO USAR PALABRAS** que se encuentren en el diccionario ni patrones de teclado, como por ejemplo *qwerty*, ni números en secuencia o repetidos. Tampoco, datos personales o que refieran a la vida cotidiana.

► **UTILIZAR** gestores de contraseñas. Algunas de las aplicaciones más populares y gratuitas son KeepassPasswordSafe, EfficientPassword Manager, KasperskyPassword Manager y ClavesPC.

► **SI LA INFORMACIÓN** requiere mucha seguridad aplicar la *Verificación de dos pasos*.

► **CONFIGURAR** las opciones de recuperación de contraseña y mantenerlas actualizadas.

Datos biométricos, lo nuevo

AUNQUE la fecha de defunción de las contraseñas no está a la vista, ya existen nuevos métodos de protección y verificación de la autenticidad de cada usuario, ligados a datos biométricos como reconocimiento dactilar, de voz y de iris. Por ejemplo, Apple lanzó este año el iPhone 5S con una aplicación de huella digital con un sensor dactilar que según los analistas marcará una tendencia que se masificará a otros dispositivos. El lector está integrado en el botón de inicio, hecho de cristal de zafiro, y el anillo que rodea la tecla detecta cuándo hay un dedo sobre el sensor. El sistema de Apple es más seguro que escribir una contraseña, pero también genera cuestionamientos sobre la intimidad de las personas. Otras dispositivos como Lenovo ThinkPad portátil y el Motorola Atrix, también están experimentando con esta tecnología.

A su vez, las empresas comienzan a sustituir las tarjetas de seguridad de ingreso a los edificios con escáneres de iris o dispositivos RFID (Identificación por Radio Frecuencia). Sin embargo, dudas sobre su seguridad ante un posible hackeo y la falta de una mayor integración con servicios *online*, ha limitado en esta etapa incipiente un uso más extendido. Esto que asegura, al menos por unos años, la necesidad diaria de seguir recordando o gestionando todas nuestras contraseñas.