La era de las contraseñas se encamina a su fin

Nuevos sistemas de seguridad en la Red buscan acabar con los fallos de las actuales claves de acceso

JORDI PÉREZ COLOMÉ

18 OCT 2018 - 16:35 CEST

Los passwords más usados hoy en internet son inmensamente fáciles de descifrar. PIXABAY

Los humanos somos muy previsibles creando contraseñas. La mayoría tiene entre 6 y 8 caracteres porque así nos lo aconsejaron. Un 55% tiene minúsculas y algún número, según esta base de datos de más 500 millones de claves filtradas. Las mayúsculas y los signos especiales aparecen solo en un 0,6% de ellos. Los números más usados al final de las letras son también inmensamente previsibles. Las tres combinaciones de dos dígitos más usadas son, al menos en esta muestra de 3 millones de contraseñas, 00, 23 y 69. Quien hace el esfuerzo de añadir tres cifras tampoco se esfuerza especialmente: 123, 000, 001, 111, 007, 666. Un algoritmo adecuado y la potencia de cálculo actual son capaces de destrozar nuestra mediocre inventiva.

Además, un 52% de los usuarios recicla sus códigos de acceso, según un estudio de la Universidad de Virginia Tech, "servicios sensibles, como webs de compra y email, tienen la mayoría de *passwords* repetidos o [levemente] modificados".

Incomprensiblemente, aún no ha habido catástrofes generalizadas que afecten a la ciberseguridad de los usuarios comunes. El email privado del autor de este artículo ha sido expuesto a ataques en bit.ly, Dropbox, LinkedIn, Tumblr y Stratford. En esta web se pueden comprobar las cuentas de correo

electrónico a las que afectan 314 *hackeos*. Aquí se puede comprobar cómo algunos códigos (es el caso de las fechas de nacimiento, por ejemplo) se repiten miles de veces en Internet.

Bill Nurr, antiguo director del National Institute of Standards and Technology de Estados Unidos, ahora jubilado con 73 años, fue quien en de 2003 aconsejó el uso de contraseñas de al menos 8 caracteres que combinaran letras y números. Pero en 2017 afirmó en una entrevista a *The Wall Street Journal* que lamentaba su propuesta: había creado un ejército en busca de combinaciones sencillas de números y letras. Lo que parecía un buen consejo se convirtió en millones de "abcd123" o "password1".

Cómo rectificar

Las fechas de nacimiento, por ejemplo, se repiten hasta la saciedad como claves de acceso

Una mejora posible es alargar esos 8 caracteres a 20 o más. Pero una sola combinación maravillosa tampoco es la solución. Mark Risher, director de seguridad de Google, ha puesto de manifiesto los riesgos de usar repetidamente una sola contraseña, por compleja que sea. Es mejor alternar *passwords* distintos, aunque sean más sencillos. "Nuestra investigación ha probado que si alguien usa el mismo código en muchas webs", afirma, "la probabilidad de ataque se multiplica por 10. Pero si alguien cae en una trampa de *phishing* [suplantación de identidad o captura fraudulenta de datos] la probabilidad de que un [nuevo] ataque tenga éxito se incrementa por 500", explica.

La solución ideal es aparentemente sencilla: una contraseña distinta y compleja para cada web. Pero aquí viene el problema: ¿quién recordará docenas de "d$%29fht_pp*!2o8"? "Escríbelo en un papel o aún mejor archívalo en un gestor de *passwords*", dice Risher.

Las grandes tecnológicas tienen sus propios gestores. Hay además apps específicas, cuyo uso no siempre es sencillo. Hay una solución intermedia aceptable: crear frases o grupos de palabras. Contraseñas de 35 caracteres (mejor con alguna ñ) son más difíciles de reventar.

Hay una solución intermedia aceptable, la de crear frases o grupos largos de palabras

El problema de fondo, sin embargo, sigue siendo el mismo: los usuarios no tienen incentivos para mejorar su seguridad porque no han visto peligrar sus datos. Esa perfección puede cambiar con el creciente refinamiento de las técnicas de *phishing*. Véase un ejemplo reciente, enviado desde la dirección comunicaciones@endesatemponegocios.coma: "Hemos detectado que una de tus facturas ha sido doblemente pagada. El origen de la mala estimación en nuestro sistema de débito automático, hemos deducido de su cuenta un importe de 765,00 EUR. En este caso debe confirmar su solicitud de reembolso". Seguía un enlace en el que se requerían los datos del destinatario. La cifra y la redacción deficiente dan motivos para sospechar de un fraude, pero el sistema es bastante más sofisticado que el de los correos que prometen beneficios millonarios por participar en operaciones ilegales (lo que se conoce como *timo del nigeriano).*

Este tipo de *phishing* tiene grados de perfección. En el reciente hackeo de 29 millones de usuarios de Facebook, los atacantes se hicieron con las cuatro últimas cifras de millones de tarjetas de crédito. No sirven para sacar dinero, pero tienen otros usos, según Risher: "Otra cosa que da bastante miedo. Algunos de los grandes *hackeos* ofrecen información que da credibilidad. Por ejemplo, los cuatro últimos dígitos de tu tarjeta. Así que te pueden escribir algo así: 'Jordi, somos el Banco Santander sobre tu tarjeta de crédito que termina en ****3456'. Eso puede ser bastante creíble incluso si no saben tu número completo de tarjeta. Ese poco que saben hacer que parezca mucho más legítimo".

El *phishing* no se dirige a nadie de forma específica. Sí el *spear phishing,* modalidad de fraude en la que se intenta entrar en cuentas concretas, en ocasiones no solo por dinero: "Los datos pueden ser más importantes que el dinero. Nuestra propia información puede ser usada para comprometer nuestras cuentas personales, organizaciones o, en casos extremos, la seguridad nacional del país", dice Michael Sirivianos, profesor en la Universidad de Tecnología de Chipre. El *spear phishing* fue el origen del *hackeo* al Partido Demócrata de Estados Unidos antes de las elecciones de Trump. O de la intrusión en Sony por parte de Corea del Norte.

A Risher no le gusta admitirlo para no dar sensación de derrota, pero una de las cosas que mejor garantizan la ciberseguridad del usuario corriente es que, como tal, no es interesante para nadie: "Espero que los lectores se lleven la impresión de que no todo es *hackeable*. Hay muchas cosas que se pueden hacer que limitan las oportunidades de que pase algo malo", dice Risher, que añade: "Aunque el porcentaje no llega a cero porque hay esa asimetría entre atacante y defensor. Como defensores tenemos que asegurarnos de que cada ventana, cada puerta, la chimenea, el sótano, todo esté cerrado. El atacante solo necesita una vía abierta para entrar. Eso es una gran ventaja, pero no significa que debas dejar la puerta sin cerrar".

El fin de todas las claves personales

Mark Risher, director de seguridad de Google. **GOOGLE**

El futuro de la contraseña es desaparecer. La seguridad en la Red será tan importante que dependerá de algo físico: una llave, el móvil. Un equipo codirigido por Sirivianos ha creado uno de estos sistemas, ReCRED, donde la seguridad depende del acceso al móvil mediante factores biométricos: huella, reconocimiento facial. "Esto pasa la carga de la autenticación del usuario al móvil que siempre llevamos encima", explica. Sirivianos cree que este sistema se generalizará en un plazo de 5 años.

Google y otras plataformas ya ofrecen el doble factor de autenticación: si se activa esta modalidad, el acceso a la cuenta de un ordenador se controla desde el teléfono móvil. Google ofrece ya su Sistema de Seguridad Avanzado, que obliga a comprar dos llaves físicas, limita las *apps* de terceros dentro del correo y trata de interceptar mensajes de suplantación de identidad.

Otro modo de dejar atrás las contraseñas será el análisis del comportamiento *online*: "Hoy se investiga en sistemas de autenticación continua, que monitorizan las acciones del usuario. Si el comportamiento difiere suficientemente de lo esperado, el sistema toma medidas", dice Andrés Marín, profesor de la Universidad Carlos III de Madrid.

La magnitud del negocio del *hackeo* es enorme. Risher no explica si hay incluso Gobiernos detrás de algunos esfuerzos criminales: "Es posible localizar dónde está esta gente, pero no merece la pena dedicar muchos recursos a localizar quién está detrás de los mismos tipos de ataques que provienen de muchos adversarios distintos". Y añade: "Es un negocio provechoso. Hay grupos donde un equipo investiga, otro trabaja con infraestructura (servidores), otros preparan los mensajes e incluso un cuarto aporta recursos humanos y salarios. Algunos tienen oficinas por todo el mundo para cubrir diferentes husos horarios", concluye Risher.

ARCHIVADO EN:

Hacker · Google · Buscadores · Delitos informáticos · Seguridad internet · Internet · Empresas · Delitos · Telecomunicaciones · Economía · Comunicaciones · Justicia