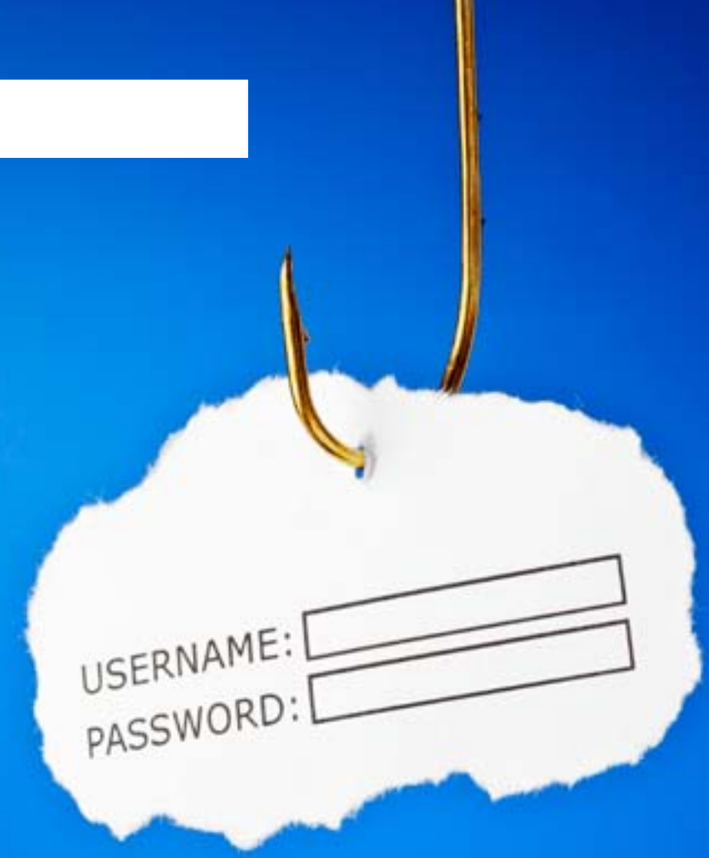
CÓMO PROTEGER SUS CUENTAS EN INTERNET



Por: Javier Méndez

En la Red somos muy vulnerables. Datos personales, información corporativa confidencial y cuentas de correo y redes sociales, entre otros, están al alcance de delincuentes y hackers si no se toman ciertas precauciones. Consejos para protegerse.

El caso del experto en seguridad informática Greg Hoglund ilustra de forma dramática cuál puede ser la consecuencia de omitir recomendaciones de seguridad sencillas, como la de crear contraseñas fuertes y no usar un mismo password para todas las cuentas en Internet.

Hoglund, fundador de la compañía estadounidense HBGary Federal, que asesora a gobiernos y empresas en temas de seguridad en Internet, notó el 6 febrero de este año que algo estaba mal cuando no pudo entrar a su cuenta de correo corporativo de Google. Alguien había tomado el control de su correo y había cambiado la contraseña.

Para cualquier persona esa es una situación complicada, pero es especialmente bochornosa para alguien que se gana la vida protegiendo a las organizaciones de acciones como esta. Hoglund pidió ayuda al soporte técnico de Google para cerrar la cuenta, pero ya era demasiado tarde: los hackers, del grupo Anonymous, se habían adueñado de 60.000 mensajes de correo personales y de su empresa, los cuales hicieron públicos en Internet.

Ellos aprovecharon una vulnerabilidad del software del sitio web de HBGary Federal y consiguieron una lista encriptada de los nombres de usuario y passwords de los empleados, que lograron decodificar porque la contraseña maestra era débil. Pero el mayor daño se produjo porque Hoglund y otros ejecutivos de su empresa habían cometido una falta imperdonable, especialmente para cualquiera que se considere experto en seguridad: habían usado las mismas contraseñas para múltiples cuentas (correo laboral, correo personal, redes sociales, etc.).

Gracias a ello, los hackers saltaron fácilmente de cuenta en cuenta. Eso no sólo les permitió burlarse de Hoglund y de otros empleados de la firma en sus propias cuentas de Twitter, sino que les dio acceso a correos en los que se revelaba que HBGary Federal había ofrecido a entidades como la Cámara de Comercio de Estados Unidos y el Bank of America el servicio de inteligencia y espionaje por Internet en contra de grupos opositores, entre ellos gente que apoyaba a WikiLeaks. Esos servicios nunca se usaron, pero el solo hecho de haberlos considerado desató un escándalo que hizo que Hoglund perdiera los contratos de varios de sus principales clientes; además, él, sus empleados y sus familias recibieron una avalancha de agresiones y amenazas –incluso de muerte– por teléfono e Internet.

La mayoría de los ataques no se enfocarán en tratar de averiguar sus contraseñas mediante avanzadas herramientas tecnológicas, sino con el más mundano recurso de aprovecharse de su ingenuidad.

Pero los hackers no se contentaron con eso. También divulgaron correos personales de Hoglund y de Aaron Barr, uno de los empleados de la empresa, con quien se ensañaron porque él había aparecido en varios medios anunciando que había descubierto las identidades de varios de los miembros de Anonymous y que pronto las daría a conocer. Los hackers publicaron fotos personales de Barr y detalles privados sobre su familia.

3.334 MILLONES DE PASSWORDS POR SEGUNDO

Hace unos meses, el blog Vijay's Tech Encounters publicó un artículo que cuenta cómo se están utilizando programas para violar contraseñas (password crackers) que se apoyan no en el poder del procesador del PC, sino en las excepcionales capacidades que tienen para esa tarea los procesadores de las tarjetas gráficas (las GPU o Unidades de Procesamiento Gráfico). Gracias a ello, el tiempo que toma averiguar una contraseña se reduce a un nivel aterrador.

En la nota se explica que averiguar una contraseña de acceso a Windows de cinco caracteres (**fjR8n**) tomó 24 segundos usando un 'ataque de fuerza bruta' con un password cracker que se apoya en el procesador convencional de un computador (a una tasa de 9,8 millones de contraseñas probadas por segundo); en cambio, usando un software que emplea el procesador gráfico el tiempo se redujo a 1 segundo (¡a una tasa de 3.334 millones de passwords por segundo!).

Cuando se alargó la contraseña a seis caracteres (**pYDbL6**) al procesador le tomó 1 hora y 30 minutos, frente a 4 segundos de la GPU. Y en un password de siete caracteres (**fh0GH5h**) el procesador gastó 4 días frente a solo 17 minutos de la GPU.

Esas cifras son preocupantes. Aunque esas contraseñas no incluyen caracteres especiales, tampoco están formadas por palabras que se encuentran en el diccionario (los 'ataques de fuerza bruta' son más difíciles y tardan más que los 'ataques de diccionario'), y posiblemente son más seguras que muchas de las claves que usted utiliza. Pero incluso con contraseñas más largas el software basado en la GPU es muy efectivo.

Por ejemplo, en una contraseña de ocho caracteres (**t6Hnf9fL**) el software para GPU tarda 18 horas (frente a un estimativo de casi año en un password cracker convencional); y en una de nueve caracteres (**kfU-64FdB8**) se demora 48 días (frente a 43 años del otro método). Solo cuando la clave llega a 10 caracteres el tiempo del cracker para GPU se vuelve excesivo: 8 años y 70 días. Sin embargo, es cuestión de tiempo para que el software y el hardware sean más potentes y empiecen a pulverizar en tiempos razonables contraseñas más largas.

De hecho, el password cracker que se utilizó para esta prueba es gratuito y se consigue en Internet; además, la GPU que se probó es la que incluye una tarjeta gráfica común, como la que tienen instalada muchos PC hoy .

El autor de este blog también hizo la prueba de disparar un ataque de fuerza bruta contra una contraseña de 10 caracteres basada solo en números (**8457317452**) y al software le tomó sólo dos segundos averiguarla. En cambio, en una clave de nueve caracteres variados (**H<k7$6fVJ**) el tiempo se eleva a siete años.

Pero Barr y el presidente de HBGary Federal todavía podían caer más bajo: desesperados por la situación, pasaron por la vergüenza de pedir clemencia a Anonymous en algunos chats de Internet. La petición no fue aceptada por los hackers, quienes respondieron publicando correos confidenciales en los que se revelaban vulnerabilidades en los sistemas de varios clientes de HBGary Federal, entre ellos empresas como Sony, Johnson & Johnson y Disney.

Barr renunció a la empresa en mayo pasado y Hoglund, quien tenía una alta reputación como experto en seguridad (él mismo era considerado un hacker, de los buenos), ahora lucha por recuperar su prestigio y el de su compañía.

SOMOS VULNERABLES

Es evidente que la agresión anterior, descrita en un artículo de la revista BusinessWeek, muestra un interés particular de los hackers por perjudicar a sus víctimas. Pero, guardadas las proporciones, esos casos no son tan infrecuentes hoy en día, ni siquiera en Colombia.

El mes pasado se conoció en el país el caso de Daniel Samper Ospina, director de la revista Soho, cuyas cuentas de correo y redes sociales fueron hackeadas por un estudiante de 23 años, quien publicó en Internet información personal de Samper y datos confidenciales de la revista; él también amañó algunos correos para dañar la imagen de Samper con información falsa, según dijo el periodista en una entrevista en radio.

No era la primera vez que este joven hacía algo parecido: se le acusa de haber penetrado en las cuentas de 116 personas, muchas de ellas políticos, periodistas y gente de la farándula. Pero el episodio en Colombia tuvo un final diferente al de HBGary Federal en Estados Unidos. Este hacker fue identificado por la Unidad de Delitos Informáticos de la Dijín y enfrenta un proceso que podría darle una pena de hasta ocho años de prisión.

Sin embargo, lo que estas dos situaciones tienen en común es que muestran el enorme grado de vulnerabilidad en el que vive cualquier usuario de Internet. Datos personales, información corporativa confidencial, mensajes de correo y cuentas de redes sociales, entre otros, están a merced de delincuentes y hackers, que los pueden usar para desprestigiar a las personas o para cometer delitos (por ejemplo, financieros).

Es innegable que algunas de estas acciones tienen éxito por el conocimiento técnico de los hackers y por la proliferación en la Red de herramientas de software que permiten concretar estos delitos. Pero también es claro que los usuarios de Internet les facilitan la vida a los delincuentes al no tomar unas medidas de precaución mínimas para proteger sus cuentas y su información personal.

Es tal el descuido que buena parte de estos ataques se concreta sin necesidad de realizar trabajo técnico; son simplemente labores de inteligencia e ingeniería social, en las que los hackers se aprovechan de la ingenuidad de las víctimas para averiguar la información que les permite penetrar en sus cuentas.

Muchos de los errores que cometen los usuarios tienen que ver con el manejo de sus contraseñas. Se crean contraseñas demasiado cortas y muy fáciles de descifrar. Además, la gente utiliza un mismo password para todas sus cuentas en la Red; eso permite que con sólo averiguar una contraseña un delincuente pueda penetrar en todas las cuentas que el usuario tiene en diversos servicios.

Los usuarios de Internet les facilitan la vida a los delincuentes al no tomar unas medidas de precaución mínimas para proteger sus cuentas y su información personal.

Otro problema está en que, aunque la contraseña no sea tan débil, a veces es posible evadirla aprovechando la función de 'pregunta secreta' que suelen tener los servicios de Internet para que las personas restablezcan su contraseña en caso de que la olviden.

Los usuarios tampoco se toman la molestia de encriptar sus documentos confidenciales, ni acatan la recomendación mil veces repetida de no entrar a sus cuentas importantes desde lugares públicos como los cafés Internet (y mucho menos realizar transacciones financieras desde allí).

Igualmente, la gente comete el pecado grave de mantener sus computadores sin antivirus (o de utilizar unos que están desactualizados); esta es, por ejemplo, una práctica común entre los usuarios de Mac. Eso hace que todas las precauciones que tengan con sus contraseñas se pierdan, ya que la falta de un antivirus permite que los delincuentes capturen datos confidenciales, entre ellos contraseñas, mediante programas malignos –los key-

loggers– que introducen fácilmente en los computadores desprotegidos.

Aunque nadie puede tener una garantía absoluta de que no sufrirá un ataque como los descritos, al menos puede reducir el riesgo de que se produzca y minimizar las consecuencias. Para ello, debe seguir algunas recomendaciones de seguridad, que explicaremos en las siguientes páginas.

LA PRINCIPAL ARMA: INGENIERÍA SOCIAL

Quizás le sorprenderá saber que la mayoría de los ataques contra sus cuentas de Internet no se enfocarán en tratar de averiguar sus contraseñas mediante avanzadas herramientas tecnológicas, sino con el más mundano recurso de aprovecharse de su ingenuidad.

"La forma más fácil de hackear a una persona es con ingeniería social", asegura Andrés Guzmán Caballero, presidente de la firma Adalid Abogados, especializada en seguridad informática y análisis forense digital (en tecnología, la ingeniería social es la práctica de obtener información confidencial o acceso a los sistemas a través de la manipulación de los usuarios).

"A veces las personas tienen contraseñas seguras; lo débil es la pregunta secreta que utilizaron cuando configuraron su cuenta de correo o de otros servicios en línea. Por eso, estos ataques siempre empiezan por la pregunta secreta, ya que es lo más fácil: es una respuesta con un dato concreto, como el nombre de una persona, una ciudad o la marca del primer carro. ¿Cuántas marcas de autos había hace unos años en Colombia?", dice Guzmán.

Es fácil ver cuán vulnerable es este recurso. Si uno entra a las opciones de configuración de Hotmail, las opciones de pregunta secreta son limitadas. Son seis: el nombre del mejor amigo de la infancia, la ocupación del padre, el nombre de la primera mascota, el profesor favorito, el personaje histórico preferido y el lugar de nacimiento de la madre. Son pocas y con una cantidad de posibles respuestas reducida. Gmail tiene alternativas parecidas, pero con una ventaja: le permite crear sus propias preguntas.

Los expertos consideran que este es un sistema débil. "Los sitios web presumen que si uno puede contestar la pregunta secreta, uno es el usuario de una cuenta. Pero muchas preguntas tienen como respuesta datos que cualquiera puede descubrir con algo de investigación. Esas preguntas, además, son poco efectivas cuando el intruso es alguien cercano a uno, como una ex esposa", dice el consultor de seguridad Mark Burnett, autor del libro Perfect Passwords.

CONTRASEÑAS QUE MILES DE PERSONAS COMPARTEN

Las contraseñas son la llave de entrada a su reino privado y a sus asuntos de trabajo. Usted las necesita para entrar a sus cuentas de correo, para acceder a Facebook y Twitter, para realizar transacciones financieras, para abrir documentos de Word o Excel que ha codificado, para entrar a Windows, etc. Por ello, es inconcebible que se utilicen claves tan débiles que sean el equivalente moderno a las llaves de la casa que se dejan bajo el tapete de la entrada. Pero eso es lo que hacen la mayoría de los usuarios.

En el 2010, la compañía de seguridad Imperva presentó un informe que mostró que la mayoría de los usuarios emplea contraseñas tan básicas que se pueden romper en pocos segundos con software especializado; de hecho, son tan predecibles que ni siquiera se necesita software porque un hacker con cierta información sobre la persona puede tratar de adivinar muchas de ellas.

Imperva analizó 32 millones de contraseñas utilizadas en Internet (estas se hicieron públicas debido a una brecha de seguridad en un servicio en línea llamado RockYou) y descubrió que los passwords más comunes son casi irrisorios y son tan predecibles que muchas personas terminan empleando los mismos. Estos son los 10 primeros: 123456 (usado por 300 mil personas), 12345, 123456789, password, iloveyou, princess, rockyou, 1234567, 12345678 y abc123. Con esas contraseñas, ¿cómo pretende uno que no le hackeen sus cuentas?

La gente crea contraseñas muy parecidas, según el consultor de seguridad Mark Burnett, quien ha estudiado varios millones de claves reales. Burnett explica en su libro Perfect Passwords que 60 por ciento de las contraseñas solo tienen letras minúsculas. Menos de 3 por ciento usan mayúsculas, y estas suelen estar solo al comienzo.

Los números también se emplean de forma predecible. Lo más común es un nombre seguido de un número, y el que más se usa es el 1. Un tercio de todas las contraseñas termina con un número, y el 10 por ciento de todos los passwords finaliza con un 1.

¿Cómo averiguan los delincuentes los datos que necesitan para contestar una pregunta secreta? John Galindo, presidente de la empresa de seguridad informática Digiware, afirma que "los ataques generalmente se basan en información previamente recogida. Para ello se meten a las páginas de las redes sociales; y la labor es aún más fácil si se trata de un personaje público, ya que hay mucha información sobre su vida en Internet".

Andrés Guzmán, por su parte, explica: "Supongamos que la pregunta secreta es el nombre de un familiar. Si ya tengo cierta información suya, lo puedo llamar y le digo que soy de su EPS. Luego de darle algunos datos para ganarme su confianza, le explico que tengo un problema con las afiliaciones y necesito que me confirme los nombres de las personas que tiene en la EPS. Ese es el trabajo que se hace en el 90 por ciento de los casos de hackeo. Solo el 10 por ciento es un trabajo técnico". Por eso, Guzmán aconseja no revelar el número del celular en las redes sociales, ya que es el primer recurso que usarán los delincuentes para contactarlo y averiguar la información que necesitan.

Utilice la opción que le permite codificar los documentos importantes o confidenciales de Word o Excel. Eso minimiza el impacto de una intrusión.

Ahora bien, ¿cómo hacen los hackers para sacar información de las redes sociales si para ello tienen que estar en su lista de amigos? Guzmán explica que ese es un trabajo de inteligencia que no es tan complicado. "Es posible crear en Facebook una identidad falsa tan bien elaborada que se tenga la seguridad de que la víctima la va a aceptar en su lista de amigos, ya sea suplantando a un conocido o creando un personaje muy atractivo del cual la persona quiera ser amiga".

Entonces, lo que se puede hacer para aumentar la seguridad de la pregunta secreta es utilizar una que tenga una gama de posibles respuestas mucho más amplia, las cuales sean más difíciles de averiguar por un tercero. Incluso, dice Mark Burnett en su libro, una buena idea es agregarle algún código secreto a la respuesta, por ejemplo, algunos dígitos al final o una combinación secreta de letras.

ARTILLERÍA PESADA: PHISHING Y KEYLOGGERS

Otros métodos para averiguar las contraseñas de las cuentas de Internet son el phishing y los keyloggers. Estos son ataques más elaborados en los que el delincuente engaña a la persona con páginas web falsas para que introduzca sus datos de forma voluntaria (phishing) o en los que envía al computador de la víctima un programa maligno (el keylogger) mediante el cual se sustrae información.

Un ejemplo común de phishing son los famosos mensajes de correo electrónico en los que supuestamente su banco le pide que actualice datos como el nombre de usuario y la contraseña. En el correo llega un enlace que en apariencia lo lleva a la página de su banco, pero que en realidad conduce a un sitio web falso creado por el delincuente.

Aunque esta técnica pareciera ser trillada, todavía hay gente que cae. Y no solamente se usa para suplantar las páginas de entidades financieras; también se emplea para averiguar contraseñas de redes sociales. Según John Galindo, de la empresa Digiware, basta con que usted le envíe a una persona algo que despierte su interés –como una invitación a probar una red social nueva– para que ella dé clic en el enlace.

De hecho, hicimos una búsqueda en Google y en segundos pudimos encontrar tutoriales en los que se enseña cómo falsificar el correo de Facebook en el cual se indica que alguien quiere ser amigo suyo; cuando la persona da clic en el enlace y trata de ingresar a Facebook, en realidad está introduciendo los datos de su cuenta en una página falsa muy parecida a la de esa red social.

Andrés Guzmán explica que "otra técnica es tomar el control del enrutador de la red inalámbrica de la víctima, el cual muchas personas dejan abierto (sin contraseña). Si yo controlo el enrutador, lo puedo configurar para que cuando alguien quiera ir al sitio web de su banco no llegue allá, sino a la página falsa de un banco que yo he creado".

Por su parte, los keyloggers son programas que, una vez penetran en su computador, graban todo lo que usted escribe en el teclado. Este software se puede introducir en el PC de la víctima mediante un archivo adjunto de correo electrónico. También se puede enviar al computador de la persona directamente, aprovechando vulnerabilidades de su sistema.

Según Andrés Guzmán, "uno puede conocer datos como qué sistema operativo tiene un usuario o cuál es su dirección IP a través de las huellas que deja su navegador en la Red; así, un hacker puede hacer un escaneo por Internet para ver si esa persona tiene puertos abiertos y de esa manera tratar de introducir el keylogger directamente".

RECOMENDACIONES PARA CREAR CONTRASEÑAS FUERTES

1. Cree contraseñas de 10 a 15 caracteres hacia arriba. Las de menor tamaño son muy vulnerables.

2. No construya sus passwords sólo con números y letras en minúscula. Agrégueles signos de puntuación, símbolos y mayúsculas.

3. No utilice palabras que se encuentran en el diccionario (ni en español ni en otros idiomas). Tampoco nombres de familiares u otros datos relacionados con su entorno.

4. No use los números de forma obvia. Por ejemplo, el 10 por ciento de las contraseñas terminan con un 1.

5. No emplee los símbolos de manera predecible. Las @ como remplazo de la letra 'a', los 3 en lugar de la 'E' y el 1 en vez de la 'l' son lugares comunes que los hackers y su software conocen.

Una vez el keylogger está en el computador del usuario, todos los datos que él escribe se le envían al hacker por Internet. John Galindo afirma que los keyloggers modernos ya no entregan una montaña de información en desorden, sino que le pueden decir al hacker que la persona entró a cierta página web y escribió tal o cual texto. Incluso, se pueden programar para que le envíen al atacante un correo cada vez que la víctima visita cierto sitio web (por ejemplo, el de Hotmail o el de un banco).

¿Cuál es la defensa ante los keyloggers? Un buen antivirus pagado. Andrés Guzmán resalta que la gente instala antivirus gratuitos y piensa erróneamente que así está protegida. "Eso es un ataque contra uno mismo. Lo que uno debe hacer es comprar un buen antivirus y pagar la actualización cada año; y no sólo para el PC, sino también para el celular y para el tablet", dice.

Bajamos la versión de prueba de un password cracker y la enfrentamos a contraseñas de documentos de Word 2010. Le tomó entre 4 y 15 segundos averiguar claves de cinco caracteres basadas solo en palabras reales; las de seis y siete caracteres cayeron antes de 30 segundos.

ATAQUES CON PASSWORD CRACKERS

Los password crackers, programas que prueban millones de contraseñas cada segundo, son otra importante arma de los hackers. Hay muchas herramientas de este tipo y algunas se consiguen fácilmente en Internet; entre las más conocidas están Cain and Abel, Hydra y John the Ripper.

Los delincuentes generalmente no tratan de averiguar las contraseñas de servicios web mediante ataques en línea basados en password crackers, ya que sitios como Hotmail o Gmail tienen una protección: se bloquean después de varios intentos fallidos. Sin embargo, es clave tener contraseñas muy fuertes para estos servicios; no solo para evitar ataques basados en ingeniería social, sino porque un hacker muy paciente podría usar una herramienta automatizada que visite un sitio cada 24 horas, pruebe unas pocas contraseñas y luego repita el proceso al día siguiente (se puede configurar el software para que los passwords que se intenten se basen en su información personal). No es habitual, pero podría pasar.

Otro método es tomar combinaciones de nombres de usuario y contraseñas comunes (las personas suelen crear passwords muy parecidos, como se explica en el recuadro 'Contraseñas que miles de personas comparten') para probarlas en cientos de servicios web con una herramienta automatizada. Como las contraseñas son tan predecibles, esta técnica, que parecería dispersa y desenfocada, suele tener un buen porcentaje de resultados exitosos.

Igualmente, se deben crear contraseñas muy fuertes para los documentos de Office que se encriptan en el PC, para los enrutadores de las redes Wi-Fi de la casa y la oficina, para acceder a Windows, para entrar a la red de la empresa y para los programas de encriptación que uno use en el PC, entre otros. Si alguien se adueña por ejemplo de sus

documentos codificados (cuando le roban un portátil o una memoria USB), su única defensa ante un password cracker será que su contraseña sea fuerte y larga. Sin embargo, esto no es lo habitual; la gente suele crear claves muy débiles y predecibles, que son fáciles de romper.

Bajamos la versión de prueba de un password cracker comercial (Passware) y la enfrentamos a contraseñas de documentos de Word 2010. Al software le tomó entre 4 y 15 segundos averiguar claves de cinco caracteres basadas solo en palabras reales; las de seis y siete caracteres cayeron antes de 30 segundos (todas las palabras estaban en minúsculas). Eso le da una idea de lo fácil que es violar un password débil. Sin embargo, cuando se crean contraseñas más largas, sin palabras reales y con caracteres especiales, estos programas reducen su efectividad.

¿Cuántos caracteres debe incluir una contraseña para que se considere sólida? Eso depende de la importancia que tenga para usted lo que está protegiendo. Yo uso contraseñas de 30 a 35 caracteres en documentos muy importantes de Office o en programas de encriptación como Steganos, y empleo claves cercanas a 20 caracteres para entrar a Windows y a las cuentas de Internet (no todos los servicios en línea permiten crearlas de esa longitud). Todas ellas son irreconocibles y las cambio de forma regular. Sin embargo, si usted no es tan quisquilloso, hágale caso a los expertos que recomiendan usar contraseñas de entre 10 y 15 caracteres.

Parecen demasiado largas, pero está en un error si cree que eso es un acto de paranoia. A medida que aumenta la potencia de los computadores, también crece la capacidad de los passwords crackers para derribar contraseñas. Así que olvídese de los expertos en seguridad que todavía le dicen que una clave de 8 o 9 caracteres es segura. Ya no lo es (ver recuadro '3.334 millones de passwords por segundo').

Nueva técnica pulveriza contraseñas

Tamaño de la contraseña	Tiempo para averiguarla con cracker convencional (tasa: 9,8 millones de passwords probados por segundo)	Tiempo con nuevo cracker basado en chip gráfico (tasa: 3.334 millones de passwords por segundo)
5 caracteres **(fjR8n)**	24 segundos	1 segundo
6 caracteres **(pYDbL6)**	1 hora y 30 minutos	4 segundos
7 caracteres **(fh0GH5h)**	4 días	17 minutos
8 caracteres **(t6Hnf9fL)**	Casi 1 año	18 horas
9 caracteres **(kfU64FdB8)**	43 años	48 días

*** Fuente: el blog Vijay's Tech Encounters.**

Por qué debe ser larga y con caracteres especiales

Tamaño de la contraseña	Tiempo que toma averiguar clave con caracteres simples	Tiempo para contraseña con caracteres especiales
8 caracteres	18 horas para la contraseña **t6Hnf9fL**	25 días para la contraseña **g&4K 3gl** (uno de los caracteres es un espacio)
9 caracteres	48 días para **kfU64FdB8**	7 años para **H<k7$6fVJ**

*** Fuente: el blog Vijay's Tech Encounters.**

**** Tiempos con un password cracker basado en GPU (los más poderosos)**

BUSQUE BUEN TAMAÑO Y VARIEDAD

Crear contraseñas fuertes y largas es una tarea a la que debe dedicar tiempo. No se trata de que escoja una contraseña para salir del paso, sino de que se tome el tiempo para construirla.

Hay muchos artículos que ofrecen recomendaciones sobre cómo crear contraseñas. En esencia, lo que le dicen es que no se deben utilizar palabras que se encuentren en un diccionario, ni nombres propios (y menos si están asociados con su entorno). Además, debe emplear números pero no escribirlos en series (123456), tiene que incluir caracteres especiales (como signos de puntuación o símbolos) y debe usar mayúsculas y minúsculas.

La razón para hacer esto es que con cada juego adicional de caracteres que use en su contraseña usted está obligando al hacker a incluir un parámetro más en el software que utiliza para romper su password; eso aumenta el tiempo que le toma averiguar su clave.

El libro Perfect Passwords explica este punto mediante un ejemplo. Un candado de los que utilizan clave suele tener tres ruedas selectoras y cada una de ellas permite escoger los números del cero al nueve. Eso da un total de 1.000 posibles combinaciones, que no es mucho. Si se construyera un candado que en lugar de utilizar sólo números también incluyera las letras de la A a la Z en cada una de las tres ruedas, el número de posibles combinaciones aumentaría a casi 50 mil.

Con las contraseñas pasa algo similar. Si usted sólo usa letras minúsculas, y encima las emplea para crear palabras que existen en un diccionario, les está facilitando la labor a los delincuentes porque un password cracker puede obtener resultados en unos pocos segundos. En cambio, si emplea símbolos, mayúsculas y números (es como aumentar el número de opciones en las ruedas selectoras de un candado), y además genera contraseñas muy largas (eso equivale a no tener solo tres ruedas en el candado, sino muchas más), está disparando el tiempo y el trabajo que les toma.

Cuando un hacker se adueña de una base de datos de contraseñas o de un documento encriptado, es posible que primero intente un 'ataque de diccionario' con el password cracker. En este tipo de procedimiento el software trata de adivinar la clave probando con todas las palabras que se encuentran en los diccionarios de varios idiomas. Además, los programas modernos permiten incluir variaciones ligeras de las palabras (por ejemplo, con números al comienzo o al final) y también se valen de listados de las contraseñas más comunes. Los ataques de diccionario toman poco tiempo y, como mucha gente utiliza los mismos passwords, se obtienen buenos resultados.

Si esa técnica no es exitosa, el hacker intentará un 'ataque de fuerza bruta'; en esta modalidad, el software trata de generar todas las combinaciones posibles de contraseñas con el tipo de caracteres que se escogen para el intento. Para reducir el tiempo que le toma al programa producir resultados, los hackers primero probarán con letras y números; no solo es más rápido, sino que la mayoría de las contraseñas únicamente incluye esos dos elementos.

Sólo si se trata de un trabajo más elaborado y se dispone de mucho tiempo, se incluirán en los parámetros del software los ataques de fuerza bruta con símbolos y caracteres especiales. Los resultados tardarán mucho más; de hecho, si

7 CONSEJOS PARA PROTEGER SUS CUENTAS EN LA RED

1. Utilice contraseñas no predecibles y extensas. Además, asegúrese de que la pregunta secreta que los sitios web le piden para restablecer su clave –en caso de que la olvide– no tenga una respuesta que un tercero pueda averiguar fácilmente. Incluso, se sugiere agregar algunos dígitos a la respuesta para aumentar la seguridad.

2. Sea desconfiado con las llamadas telefónicas que le hacen para solicitarle información personal. Ese es el método que usan muchos delincuentes para obtener información que les permita acceder a sus cuentas de Internet.

3. De nada le sirve tener contraseñas seguras si su computador está desprotegido por falta de un buen antivirus. Si su antivirus es débil, le pueden introducir en el PC un keylogger, un programa que graba todo lo que usted escribe en el teclado (entre eso sus claves). Los antivirus gratuitos no son tan seguros como los pagados.

4. Mantenga todo su software actualizado y con los últimos parches de seguridad (sistema operativo, navegador, aplicaciones). Las vulnerabilidades del software permiten que los delincuentes penetren en su PC e instalen programas malignos. Las versiones recientes de Windows son más seguras que las antiguas.

5. Cree una contraseña fuerte para el enrutador de su red Wi-Fi, otra para entrar a su red inalámbrica y utilice la tecnología de encriptación más fuerte que sea posible en su red Wi-Fi (generalmente, WPA2). Los delincuentes pueden capturar el tráfico de su red si no lo hace.

6. Tenga cuidado con todos los enlaces que le lleguen en mensajes de correo electrónico y que lo inviten a introducir los datos de sus cuentas en línea. Esta técnica, conocida como phishing, no sólo se usa para capturar datos financieros, sino también los de redes sociales. Un mensaje que lo invita a aceptar a un amigo en Facebook bien puede ser una trampa.

7. Utilice la opción que le permite codificar los documentos importantes o confidenciales de Word o Excel. Eso minimiza el impacto de una intrusión. Encripte esos documentos con contraseñas fuertes y largas. Y no confíe en la tecnología de codificación de las versiones antiguas de Office; use versiones recientes de esos programas.

su contraseña es suficientemente larga y compleja, el password cracker pasará de entregar resultados en horas o días a ofrecerlos en meses o años. De ahí la importancia de incluir esos elementos en las contraseñas.

CÓMO CONSTRUIR LA CONTRASEÑA

La meta, entonces, es crear una contraseña larga y compleja, pero sin correr el riesgo de que se le olvide. Para ello se emplean técnicas que le permiten recordar con cierta facilidad contraseñas elaboradas.

Por ejemplo, una contraseña podría estar formada por las primeras letras de cada palabra en un par de líneas de una canción (como una especie de acróstico). Una canción del grupo español 'El último de la fila' tiene un pedazo que dice así: "convertidos en paganos, subiremos a algún monte a meditar, a adorar becerros de oro, y a quemar barras de incienso en un altar…". Tomando las primeras letras de cada palabra, eso formaría la siguiente contraseña: **cepsaamamaabdoyaqbdieua** (de 23 caracteres).

Ese es un password completamente ininteligible y es largo. Sin embargo, está formado sólo por letras minúsculas, por lo que debe hacerse más fuerte. Hay muchas opciones para ello, y la idea es que usted cree un sistema propio.

Por ejemplo, uno podría agregar comas en los lugares donde la canción tiene cortes (**cep,saamam,aabdo, yaqbdieua**), podría cambiar todas las letras 'a' por el símbolo # (**cep,s##m#m,##bdo,y#qbdieu#**), podría remplazar las letras 'e' por el número 1 (**c1p,s##m#m,##bdo,y#qbdi1u#**) y podría poner en mayúsculas las dos letras 'm' (**c1p,s##M#M,##bdo,y#qbdi1u#**).

Esta es una contraseña fuerte de 26 caracteres, el tipo de password que uno usaría para un programa de encriptación que protege contenido muy relevante o para un documento de Office con cosas privadas; pero si se trata de la contraseña que usa todos los días en su cuenta de correo, podría quitarle un pedazo a la canción y dejarla hasta la palabra "oro" así: **c1p,s##M#M,##bdo** (queda de 16 caracteres).

A veces las personas tienen contraseñas seguras; lo débil es la pregunta secreta que utilizaron cuando configuraron su cuenta de correo o de otros servicios en línea.

A un atacante le tomará años romper esta contraseña con un password cracker. Y aun así, pese a su aparente complejidad, es una contraseña que se puede recordar fácilmente. Como usará un par de líneas de una canción que ya se sepa, lo único que debe recordar es qué caracteres cambia o agrega: en este caso, el símbolo # por la letra **a**, el número **1** por la **e**, las M en mayúsculas y las comas entre las líneas de la canción.

¿No podría simplemente dejar la contraseña larga pero con los caracteres sencillos? No debería. Crear una contraseña que sólo incluya un juego de caracteres es un riesgo grande. El blog Vijay's Tech Encounters hizo la prueba de disparar un ataque de fuerza bruta contra una contraseña de 10 caracteres basada solo en números (**8457317452**) y al software le tomó sólo dos segundos averiguarla (ver recuadro '3.334 millones de passwords por segundo').

En cambio, violar una contraseña de ocho caracteres basada en varios tipos de elementos (**g&4K 3gl**) tarda 25 días con el mismo software (hay un espacio entre la **K** y el **3**, otro recurso útil al crear passwords); y cuando se agrega una letra más para crear una clave de nueve caracteres variados (**H<k7$6fVJ**) el tiempo se eleva a siete años.

Con el mismo software, una contraseña de ocho caracteres basada únicamente en letras y números (**t6Hnf9fL**) se descubre en solo 18 horas; y una de nueve caracteres (**kfU64FdB8**) se averigua en 48 días. Como verá, los caracteres especiales y símbolos marcan una diferencia grande, lo mismo que la extensión.

CREE UN SISTEMA PROPIO

El sistema para crear contraseñas debe ser personal, algo que sólo usted conozca, y no tiene que estar atado a canciones; pueden ser frases, partes de libros, etc., pero lo importante es que no sean cosas relacionadas con su entorno o que otra gente sepa sobre usted.

Otra opción para crear contraseñas es usar palabras completas, pero deformándolas con símbolos: por ejemplo, puede emplear dos o tres palabras seguidas, que no estén relacionadas entre sí ni tengan nada que ver con usted (nunca use nombres de familiares, ni el de su mascota, ni la ciudad donde nació, ni su fecha de nacimiento, etc.).

Suponga, por ejemplo, que emplea las palabras 'absurdo aburrido', pero luego cambia las letras 'r' por un símbolo (/), las letras 'b' por un número (8), deja en mayúsculas las letras O y mete una de las palabras entre paréntesis. Quedaría así: **a8su/dO(a8u//idO)**. Eso le da una clave de 17 caracteres que no es fácil averiguar con un ataque de fuerza bruta.

Después de crear la contraseña, escríbala varias veces hasta que se acostumbre a digitarla en el teclado. Al comienzo le costará trabajo, pero en unos días la escribirá rápido. Sin embargo, si ve que algunos de los caracteres que remplazó quedan en lugares muy lejanos del teclado y eso le impide escribirlos de forma fluida, podría cambiarlos por otros. Lo que no debe hacer es caer en lugares comunes: por ejemplo, remplazar las 'a' por @ o los '3' por E. Todo el mundo hace eso, y los hackers y su software lo saben.

De esta forma puede crear varias contraseñas, unas más complejas y extensas que otras dependiendo del servicio o la información que quiera proteger. Mark Burnett recomienda en el libro Perfect Passwords algo con lo que no todos los expertos en seguridad estarían de acuerdo: anotar una contraseña nueva y guardarla unos días mientras la memoriza (por supuesto no en un papel pegado a su monitor, sino en un lugar muy seguro, como un documento encriptado en su PC).

Yo no lo haría, pero quizá sí pueda escribir en un documento encriptado pistas que le permitan recordar las claves que no usa tan seguido, sin anotar la contraseña completa. Otra opción es comprar un programa administrador de contraseñas, que guarda e introduce sus diversos passwords cuando se necesitan (estos se protegen bajo una sola contraseña maestra).

Es evidente que las contraseñas mencionadas en los ejemplos anteriores no son tan fáciles de escribir ni recordar como su **TeamoMaria** (siendo María el nombre de su esposa, su amante o su hija), pero puede estar seguro de que usar esta última contraseña es como dispararse en un pie y no lo protegerá gran cosa el día que alguien quiera entrar a sus cuentas o abrir sus documentos privados.

CÁMBIELAS Y NO USE LA MISMA

Cuando uno crea contraseñas fuertes, fáciles de recordar y que además se escriben con fluidez, puede empezar a sentir apego por ellas. Sin embargo, otra recomendación importante es precisamente que cada cierto tiempo cambie esas claves que con tanto juicio construyó por otras nuevas.

Una razón es que uno puede tener contraseñas muy fuertes, pero nunca sabe qué tan seguro es el servicio en donde se utilizan. El mejor ejemplo está en el escándalo que se produjo cuando varios servicios de Sony, entre ellos la red de juegos PlayStation Network, fueron penetrados por los hackers a comienzos de este año: uno de los descubrimientos más sorprendentes fue que Sony almacenaba las contraseñas en archivos de texto simple dentro de sus servidores.

Eso significa que los passwords que se robaron ni siquiera tuvieron que ser decodificados, sino que ahora son públicos y están en poder de delincuentes de Internet. Si eso sucede en los sitios de una compañía tan prestigiosa como Sony, ¿qué se puede esperar de muchos de los otros servicios que usamos en la Red?

Mark Burnett explica que la frecuencia más adecuada para cambiar una contraseña depende de qué tan fuerte sea el password, qué tan importante sea la información que protege con él y qué tan bien protegido esté el sistema que lo almacena.

Una contraseña débil, dice Burnett, no es adecuada ni un mes, mientras que una fuerte se puede mantener varios meses. Por otra parte, que algunas cuentas queden comprometidas puede tener consecuencias devastadoras, mientras que perder otras quizá no sea muy importante. "Algunas cuentas se pueden dejar durante un año sin cambiar la contraseña, pero en otras se debe cambiar cada tres meses", dice.

John Galindo, de la empresa de seguridad Digiware, aconseja analizar todos los servicios que uno usa y dividirlos en varios niveles: por ejemplo, un nivel superior en el que estén las cuentas de correo, las de entidades financieras y las de redes sociales, que deben tener contraseñas muy sólidas y que se cambien de manera constante; otro en el que estén archivos importantes que se almacenan encriptados en su PC, los cuales requieren passwords fuertes pero que pueden dejarse más tiempo; y un nivel inferior en el que estén las claves de servicios menos importantes y en donde usted no tenga datos sensibles.

Uno o dos caracteres más que agregue a una contraseña pueden ser la diferencia entre tener una clave que se puede violar en días mediante software a tener una que tarda años.

Es vital que no caiga en la tentación de utilizar una misma contraseña para todas sus cuentas y servicios. Como se explicó al comienzo de este artículo, eso tiene un riesgo grande: que se adueñen de todas sus cuentas con sólo descubrir una clave. Lo preocupante es que es una práctica común. Un estudio de la firma BitDefender, presentado a mediados del 2010, mostró que 75 por ciento de las personas usa la misma contraseña de su correo para su cuenta de Facebook.

Esa compañía se basó para este informe en los passwords robados y filtrados en diversos servicios de Internet. Por ello, fue inquietante otro dato del estudio: que 87 por ciento de los nombres de usuario y las contraseñas analizadas todavía se estaban empleando en cuentas activas (otro ejemplo de por qué se deben cambiar las contraseñas de manera regular).

"Todas las redes sociales están pegadas al correo electrónico. Y si averiguo su clave de correo, puedo entrar a todos sus servicios. Si puedo ingresar a su correo, puedo hacer lo que sea de ahí hacia abajo", concluyó Andrés Guzmán.