AYUDE A PROTEGER SU INFORMACIÓN PERSONAL CON CONTRASEÑAS SEGURAS

Las contraseñas son las claves que utiliza para obtener acceso a información personal que ha almacenado en su equipo y en sus cuentas en línea.
Si algún delincuente o un usuario malintencionado consigue apoderarse de esa información, puede utilizar su nombre para abrir nuevas cuentas de tarjetas de crédito, solicitar una hipoteca o suplantarle en transacciones en línea. En muchos casos, no llegaría a darse cuenta de un ataque de ese tipo hasta que fuera demasiado tarde.

Por suerte, no es difícil crear contraseñas seguras y mantenerlas bien protegidas.

Qué hace segura a una contraseña

Para un atacante, una contraseña segura debe parecerse a una cadena aleatoria de caracteres. Puede conseguir que su contraseña sea así si se guía por los siguientes criterios:
Que no sea corta. Cada carácter que agrega a su contraseña aumenta exponencialmente el grado de protección que ofrece ésta. Las contraseñas deben tener 8 caracteres como mínimo; 14 caracteres o más sería lo ideal.
Muchos sistemas también admiten el uso de la barra espaciadora para las contraseñas, de modo que pueden crearse frases compuestas de varias palabras (una frase codificada). Por lo general, una frase codificada resulta más fácil de recordar que una contraseña simple, además de ser más larga y más difícil de adivinar.
Combine letras, números y símbolos. Cuanto más diversos sean los tipos de caracteres de la contraseña, más difícil será adivinarla. Entre otros detalles importantes cabe citar los siguientes:

- Cuantos menos tipos de caracteres haya en la contraseña, más larga deberá ser ésta. Una contraseña de 15 caracteres formada únicamente por letras y números aleatorios es unas 33.000 veces más segura que una contraseña de 8 caracteres compuesta de caracteres de todo tipo. Si la contraseña no puede contener símbolos, deberá ser considerablemente más larga en caso de que se desee conseguir el mismo grado de protección. Una contraseña ideal combinaría una mayor longitud y distintos tipos de símbolos.
- Utilice todo tipo de teclas, no se limite a los caracteres más comunes. Los símbolos que necesitan que se presione la tecla "Mayús" junto con un número son muy habituales en las contraseñas. Su contraseña será mucho más segura si elige entre todos los símbolos del teclado, incluidos los de puntuación que no aparecen en la fila superior del teclado, así como los símbolos exclusivos de su idioma.

Utilice palabras y frases que le resulte fácil recordar, pero que a otras personas les sea difícil adivinar. El medio más sencillo de recordar sus contraseñas y frases codificadas consiste en anotarlas. Al contrario que lo que se cree habitualmente, no hay nada malo en anotar las contraseñas, si bien estas anotaciones deben estar debidamente protegidas para que resulten seguras y eficaces.

Por lo general, las contraseñas escritas en un trozo de papel suponen un riesgo menor (sobre todo si hablamos de Internet) que un administrador de contraseñas, un sitio Web u otra herramienta de almacenamiento basada en software.

Cree una contraseña segura y fácil de recordar en 5 pasos.

Siga estos pasos para crear una contraseña segura:

1. Piense en una frase que pueda recordar. Ésta será la base de su contraseña segura o frase codificada. Piense en una frase que pueda memorizar sin problemas, como "Mi hijo Ángel tiene tres años".

2. Compruebe si el equipo o el sistema en línea admite directamente la frase codificada. Si puede utilizar una frase codificada (con espacios entre caracteres) en el equipo o en el sistema en línea, hágalo.

3. Si el equipo o el sistema en línea no admite frases codificadas, conviértalas en contraseñas. Utilice la primera letra de cada palabra de la frase que ha creado para definir una palabra nueva sin sentido. Si tomamos la frase del ejemplo anterior, tendríamos: "mhátta".

4. Aumente la complejidad combinando mayúsculas, minúsculas y números. También resulta de utilidad cambiar letras o cometer errores ortográficos voluntariamente. Por ejemplo, en la anterior frase codificada, considere la posibilidad de escribir incorrectamente el nombre Ángel o de sustituir la palabra "tres" por el número 3. Existen muchas posibilidades de sustitución. Por otra parte, cuanto más larga sea la frase, más compleja podrá ser la contraseña. La frase codificada podría convertirse finalmente en "Mi Hijo Áng3l tiene 3 añiOs". Si el equipo o el sistema en línea no admite frases codificadas, utilice la misma técnica para la contraseña abreviada. El resultado podría ser una contraseña como "MhÁt3a".

5. Por último, realice sustituciones con algunos caracteres especiales. Puede utilizar símbolos que parezcan letras, combinar palabras (quitar espacios) y recurrir a otros medios que permitan crear contraseñas más complejas. Mediante estos trucos, podemos crear una frase codificada como "MiHiJo @ng3l ti3n3 3 añiO$" o una contraseña abreviada (con las primeras letras de cada palabra) como MiHi@t3a.

Estrategias que deben evitarse con respecto a las contraseñas

Algunos métodos que suelen emplearse para crear contraseñas resultan fáciles de adivinar para un delincuente. A fin de evitar contraseñas poco seguras, fáciles de averiguar:

- No incluya secuencias ni caracteres repetidos. Cadenas como "12345678", "222222", "abcdefg" o el uso de letras adyacentes en el teclado no ayudan a crear contraseñas seguras.
- Evite utilizar únicamente sustituciones de letras por números o símbolos similares. Los delincuentes y otros usuarios malintencionados que tienen experiencia en descifrar contraseñas no se dejarán engañar fácilmente por reemplazos de letras por números o símbolos parecidos; por ejemplo, 'i' por '1' o 'a' por '@', como en "M1cr0$0ft" o en "C0ntr@señ@". Pero estas sustituciones pueden ser eficaces cuando se combinan con otras medidas, como una mayor longitud, errores ortográficos voluntarios o variaciones entre mayúsculas y minúsculas, que permiten aumentar la seguridad de las contraseñas.
- No utilice el nombre de inicio de sesión. Cualquier parte del nombre, fecha de nacimiento, número de la seguridad social o datos similares propios o de sus familiares constituye una mala elección para definir una contraseña. Son algunas de las primeras claves que probarán los delincuentes.
- No utilice palabras de diccionario de ningún idioma. Los delincuentes emplean herramientas sofisticadas capaces de descifrar rápidamente contraseñas basadas en palabras de distintos diccionarios, que también abarcan palabras inversas, errores ortográficos comunes y sustituciones. Esto incluye todo tipo de blasfemias y cualquier palabra que no diría en presencia de sus hijos.
- Utilice varias contraseñas para distintos entornos. Si alguno de los equipos o sistemas en línea que utilizan esta contraseña queda expuesto, toda la información protegida por esa

contraseña también deberá considerarse en peligro. Es muy importante utilizar contraseñas diferentes para distintos sistemas.

- Evite utilizar sistemas de almacenamiento en línea. Si algún usuario malintencionado encuentra estas contraseñas almacenadas en línea o en un equipo conectado a una red, tendrá acceso a toda su información.

Opción de "contraseña en blanco"

- Una contraseña en blanco (ausencia de contraseña) en su cuenta es más segura que una contraseña poco segura, como "1234". Los delincuentes pueden adivinar fácilmente una contraseña simple, pero en equipos que utilizan Windows XP no es posible el acceso remoto a una cuenta a través de una red o de Internet, por ejemplo. (Esta opción no está disponible para Microsoft Windows 2000, Windows Me o versiones anteriores). Puede optar por utilizar una contraseña en blanco en la cuenta del equipo si se cumplen estos criterios:
- Tiene sólo un equipo, o bien tiene varios equipos pero no necesita obtener acceso a la información de un equipo desde otros.
- El equipo es físicamente seguro (confía en todas las personas que tienen acceso físico al equipo).

No siempre es buena idea utilizar una contraseña en blanco. Por ejemplo, es probable que un equipo portátil que lleve consigo no sea físicamente seguro, por lo que en ese caso debe utilizar una contraseña segura.

Cómo obtener acceso a las contraseñas y cambiarlas

Cuentas en línea

En los sitios Web existen directivas de diversos tipos que rigen cómo pueden obtener los usuarios acceso a sus cuentas y cambiar sus contraseñas. En la página principal del sitio, busque un vínculo (como "mi cuenta") que le lleve a un área especial desde la que se puedan administrar las contraseñas y las cuentas.

Contraseñas para el uso de equipos

Los archivos de Ayuda del sistema operativo suelen proporcionar información acerca de cómo crear, modificar y obtener acceso a cuentas de usuario protegidas con contraseña, así como de qué manera requerir protección con contraseña cuando se inicia el equipo. También puede buscar esa información en línea en el sitio Web del fabricante del software.

Mantenga en secreto las contraseñas

Cuide de sus contraseñas y frases codificadas tanto como de la información que protegen.

- No las revele a nadie. No deje sus contraseñas a la vista de familiares o amigos (sobre todo de los niños), ya que podrían facilitarlas de buena fe a personas menos merecedoras de confianza. Las contraseñas que deba compartir (por ejemplo, la de una cuenta corriente en línea con otros titulares, como su cónyuge) constituyen las únicas excepciones.
- Proteja las contraseñas registradas. Tenga precaución acerca de dónde guarda las contraseñas que registre o anote. No deje constancia de esas contraseñas en ningún lugar en el que no dejaría la información que protegen.
- No facilite nunca su contraseña por correo electrónico ni porque se le pida por ese medio. Desconfíe de cualquier mensaje de correo electrónico en el que se le solicite la contraseña o se le indique que debe visitar un sitio Web para comprobarla. Casi con total seguridad se

trata de un fraude. Esto incluye solicitudes de empresas y personas de confianza. El correo electrónico se puede interceptar en tránsito, y un mensaje en el que se solicite información podría no proceder realmente del remitente que supuestamente envía el mensaje. En las estafas de "phishing" a través de Internet, los timadores pueden utilizar mensajes de correo electrónico fraudulentos para convencerle de que revele nombres de usuario y contraseñas y robarle datos de identidad.

- Cambie sus contraseñas con regularidad. Esto puede ayudar a despistar a los delincuentes y a otros usuarios malintencionados. El nivel de seguridad de su contraseña contribuirá a prolongar la vigencia de ésta. Una contraseña que tenga menos de 8 caracteres no debe mantenerse durante un período superior a una semana, mientras que una contraseña de 14 caracteres o más (y que cumpla las otras normas indicadas anteriormente) puede mantenerse sin problemas durante varios años.
- No escriba contraseñas en equipos que no controla. Los equipos que se encuentran en lugares como cibercafés, aulas de informática, entornos compartidos, sistemas de quiosco, salas de conferencias y terminales de aeropuertos deben considerarse no seguros para cualquier uso personal que no sea una exploración de Internet anónima. No utilice estos equipos para consultar correo electrónico en línea, comunicaciones de chat, comprobación de estados de cuentas bancarias, correo electrónico de empresa ni para utilizar ninguna cuenta que requiera un nombre de usuario y una contraseña. Los delincuentes pueden adquirir por muy poco dinero dispositivos de registro de pulsaciones que se instalan en tan sólo unos instantes. Estos dispositivos permiten a usuarios malintencionados recopilar a través de Internet toda la información que se ha tecleado en un equipo (las contraseñas y las frases codificadas son tan valiosas como los datos que protegen).

Qué debe hacer si le roban una contraseña

Asegúrese de supervisar toda la información que protege con contraseñas, como los extractos mensuales, los informes de crédito, las cuentas para compras en línea, etc. Las contraseñas seguras y fáciles de recordar pueden ayudarle a protegerse de fraudes y robos de datos de identidad, pero no ofrecen una plena garantía. Independientemente del nivel de seguridad de su contraseña, si alguien consigue obtener acceso al sistema en el que se encuentra almacenada, dispondrá de su contraseña. Si detecta alguna actividad sospechosa que pueda indicar que alguien ha tenido acceso a sus datos, avise a las autoridades cuanto antes.

Fuente: http://www.microsoft.com