reconocer su entorno y ejecute frecuentemente programas antivirus y antiespionaje actualizados.

Perfiles de contraseñas

La creación de perfiles implica la realización de una conjetura fundamentada a partir de la recopilación de información personal y datos personales sobre la persona que posee la contraseña. En muchos casos nuestras contraseñas reflejan algo que nos resulta fácil de recordar: año de nacimiento, nombre de un familiar o un amigo, ciudad de nacimiento, equipo de fútbol favorito, etc. Los creadores de perfiles toman nota de estos y otros datos similares. Si es alguien que tiene acceso a su oficina, también puede ver los libros que tiene en su biblioteca. Sea cual sea el sistema que utilice para crear sus contraseñas se le puede excusar (¡al menos, hasta que termine de leer este capítulo!), ya que la capacidad de recordad muchas contraseñas diferentes que no tengan relación con usted y sean difíciles de memorizar es limitada. Sin embargo, adivinar la contraseña mediante la posesión de información personal sobre el usuario sigue siendo el método más habitual de comprometer un sistema y el de mayor éxito para los pirata informáticos motivados.

—

Muchos sistemas de contraseñas en Internet le ofrecen la opción de recuperar su contraseña a condición de que responda a una "pregunta secreta" previamente establecida. Por alguna razón inexplicable, estas preguntas secretas (que se establecen al crear una cuenta) siempre tienen algo que ver con el nombre de su mascota o de su primera escuela o el apellido de soltera de su madre. Eso facilita muchísimo las cosas a los creadores de perfiles. Ni siquiera tendrán que adivinar su contraseña; simplemente, responden a la pregunta secreta correctamente y reciben su contraseña en un correo electrónico. Si alguna vez se le pide crear un mecanismo de recuperación de la contraseña que consista en responder a una sencilla pregunta sobre su vida personal no lo use. Si es un requisito para finalizar el proceso de registro, simplemente escriba algo ininteligible. No se fíe del proceso de recuperación mediante una pregunta secreta para recordar una contraseña que ha olvidado.

►Contraseñas personales son fáciles de adivinar

Ingeniería social

Muchas personas han sido engañadas para revelar sus contraseñas a través de situaciones y preguntas astutamente creadas. Puede ocurrir que le llame su (supuestamente) proveedor de Internet y le diga que están mejorando sus servidores y necesitan su contraseña para asegurarse de que no pierda ningún correo electrónico en el proceso. Alguien podría hacerse pasar por un colega de otra filial de su ONG y solicitar la contraseña para acceder a la cuenta de correo electrónico común, porque la persona que la conoce está enferma y hay que enviar algo urgente. Este método se conoce como "ingeniería social". Ha habido numerosos casos de empleados que revelaron información que podía causar daño, simplemente porque fueron engañados. Para los piratas informáticos sigue siendo un método eficaz para intentar acceder a un sistema.
Nadie debería revelar ninguna información relacionada con un ordenador (sobre

19
Good advice from Steven Murdoch, a researcher in the Security Group of the University of Cambridge: is to verify the person's name and affiliation, then look up their phone number in a trustworthy directory and call them back

todo las contraseñas y códigos de acceso) por teléfono ni a alguien cuya identidad no pueda verificar[17].

Fuerza bruta

La fuerza bruta es la práctica de adivinar la contraseña mediante el uso de todo tipo de combinaciones posibles. Podría significar el uso de una versión electrónica de un diccionario para probar cada palabra contenida en él. Puede parecer una tarea larga para un ser humano, pero para un ordenador es cuestión de segundos. Si su contraseña es una palabra ortográficamente correcta de un diccionario puede verse comprometida por un ataque de fuerza bruta en cuestión de minutos.

¿Tal vez utiliza como contraseña los primeros versos de una de las de 1.000 canciones o poemas más famosos? El mundo digital es cada vez más amplio y creciente con la transferencia de la literatura y el pensamiento mundiales a Internet. Existen compilaciones electrónicas de las obras de la literatura, y también pueden usarse para romper su contraseña, de modo que debería replantearse el usar una contraseña en lenguaje natural (una frase inteligible o famosa, una combinación de palabras o una frase completa).

—

Algunos sistemas de contraseñas están protegidos contra ataques de fuerza bruta. Podemos tomar como un ejemplo un cajero automático o un teléfono móvil: a pesar de que su contraseña sea una simple combinación de cuatro dígitos el sistema se apagará después de tres intentos incorrectos.

LA CREACIÓN DE CONTRASEÑAS

Métodos mnemotécnicos

Existen diversos métodos para crear contraseñas que sean difíciles de romper y fáciles de recordar para nosotros. Un método popular es el de la mnemotécnica (un método o sistema para mejorar la memoria, como una rima o un acrónimo[18]). Tomemos una frase común:

"¿Ser o no ser? Esa es la cuestión." (*Hamlet,* Shakespeare)

La podemos convertir a "SRonSR?SIaC".

En este ejemplo, hemos sustituido las palabras con una letra que suena similar, poniendo los sustantivos y verbos en letras mayúsculas y el resto de palabras en minúsculas. O, por ejemplo:

"Soñé que todos los hombres nacían iguales." (Martin Luther King)

"SÑqtlHMsNC="

Parece que sea una contraseña relativamente aleatoria y no es tan difícil de recordar porque usted sabe el truco de cómo fue formada. Otras sugerencias son sustituir por números las letras que tengan un aspecto similar a éstos

l, i, l, t = 1; o,O = 0; s, S = 5,2) o abreviar palabras usando números, letras y signos

("No más problemas" = "No+proble+";

"Cansados por el estrés" = "Knsa2?Ls3").

17
Un buen consejo de Steven Murdoch, un investigador del Grupo de Seguridad de la Universidad de Cambridge, es que compruebe el nombre y la afiliación de la persona, después busque su número de teléfono en un directorio de confianza y le devuelva la llamada.

18
WordNet, de David Slomin y Randee Tengi.