PUCMM
Pontificia Universidad Católica
Madre y Maestra

Departamento de Tecnologías de la Información
Unidad de Administración de Redes (UAR)

Consejos para proteger tus contraseñas

Una de las técnicas más utilizadas por los intrusos para obtener acceso no autorizado a los sistemas de las empresas es el **descubrimiento de las contraseñas débiles**, ya que si se tiene acceso a la contraseña del usuario, se puede acceder a los sistemas con los mismos privilegios y permisos que el usuario utilizado.

¿Cómo protegernos?

El primer paso para evitar que alguien pueda obtener contraseñas con facilidad es utilizar contraseñas complejas.

¿Qué son las contraseñas complejas?

Una contraseña compleja es aquella que no puede ser adivinada fácilmente o que no puede ser obtenida por un ataque de predicción en un período de tiempo razonable. Para este motivo, la contraseña ***no puede ser una palabra del diccionario completa, ni un nombre común, ni su nombre de usuario, ni fechas de acontecimientos importantes, ni el nombre de su mascota, familiar, empresa***, *etc*.

> *Por ejemplo, "contraseña", "password", "12345678", "Juan", son contraseñas débiles y presas fáciles para un atacante.*

Características de una contraseña compleja

- ☞ Tiene por lo menos ocho (8) caracteres de longitud.
- ☞ No contiene nombre de usuario, nombre real o nombre de la empresa.
- ☞ No contiene una palabra del diccionario completa.
- ☞ Cada contraseña nueva es muy diferente de las contraseñas anteriores. Las contraseñas incrementales (como Contraseña1, Contraseña2, Contraseña3...) no son fuertes.
- ☞ Contiene por lo menos un caracter de cada uno de los cuatro grupos siguientes:

GRUPO	EJEMPLOS
Letras mayúsculas	**A, B, C...**
Letras minúsculas	**a, b, c...**
Números	**0, 1,2, 3, 4, 5, 6, 7, 8, 9**
Los símbolos que se encuentran en el teclado (caracteres del teclado que no se definen como letras o números)	**`~! @ # $% ^ & * () _ + - = [] | \: "'<>?,. /**

- ✓ *Un ejemplo de una contraseña segura es* ***J*p2leO4>F***

¿Por qué utilizar contraseñas complejas?

Es mandatorio para las empresas y organizaciones utilizar contraseñas complejas debido a la facilidad con la que los "hackers" pueden obtener contraseñas de los usuarios. Existen diversas herramientas que permiten a los intrusos obtener las credenciales de un usuario, entre las cuales se destacan:

- **Programas basados en predicción:** diseñados para predecir las contraseñas que contienen las palabras usuales basadas en la información de un usuario (fecha de nacimiento, nombre de hijos, nombre de mascotas, direcciones, nombre de familiares, etc.).
- **Programas basados en diccionario:** utilizando el nombre de usuario buscan cada palabra del diccionario esperando encontrar una coincidencia. Esto incluye palabras largas y en otro idioma (siendo que las computadoras pueden procesar millones de operaciones por segundo).

¿Cómo hacerlo?

La forma más sencilla para emplear contraseñas complejas es utilizar palabras recordables y cambiando las vocales por símbolos y números, como se describe a continuación:

Usando las palabras "Ventana" y "Teléfono" (el primer caracter de cada palabra se ha colocado en letra mayúscula). Al unir ambas palabras resulta la clave "**VentanaTelefono**". Esta aún no es una contraseña segura. Para hacerla más compleja y difícil de adivinar, se sustituyen las vocales por los siguientes números y símbolos:

e → 3
a → @
o → 0

El resultado de este ejercicio sería la siguiente clave: ***V3nt@n@T3l3f0n0***, la cual es más compleja y difícil de adivinar para un atacante o software dañino.

Nunca divulgues tu contraseña

Seguir los siguientes consejos contribuye a mejorar la seguridad:

- ☞ Nunca digitar la contraseña en un sitio web que no sea seguro (Verificar bien la dirección web antes de ingresar cualquier información)
- ☞ Nunca compartir tu contraseña con nadie
- ☞ Nunca enviar la contraseña vía email