Generar Contraseñas Fuertes para la Gestión de Efectivo de TTS

Las contraseñas se han convertido en una parte integral de nuestras vidas, ya sea al iniciar las sesiones en nuestras computadoras, nuestra banca online, correo electrónico personal e incluso en nuestros teléfonos. La fuerza de la contraseña es un componente importante al protegerse contra el fraude, pero un número significativo de usuarios online continúan utilizando contraseñas predecibles.

Contraseñas Comunes

Las violaciones de datos han sido noticia frecuente durante 2016 y 2017. Aunque teóricamente existen muchas posibilidades para una contraseña, investigaciones demuestran que las 25 contraseñas más comúnmente utilizadas representan el 50% de una muestra de 10 millones de contraseñas.[1] Estas contraseñas comunes son las primeras que prueba un estafador, y utilizarlas lo pone a usted en riesgo.

Como Atacan los Estafadores

Es mucho más fácil crear una contraseña segura si Ud comprende cómo podría intentar hackear su cuenta un ciber delincuente. El proceso de hackeo se ha industrializado y la mayoría de las violaciones se realizan ahora con software automatizado.

Los programas de hackeo comienzan intentando con las contraseñas más utilizadas, previo a probar con las palabras y frases comunes, como pueden ser los nombres de personas, lugares y equipos deportivos. Luego continua buscando con todas las palabras en el diccionario para, finalmente, intentar millones de combinaciones de caracteres aleatorios, hasta que la contraseña se descifra o el hacker desvía su atención hacia un objetivo más fácil.

[1] http://www.telegraph.co.uk/technology/2017/01/16/worlds-common-passwords-revealed-using/

Los ejemplos debajo ilustran cuanto le llevaría a un hacker con una computadora domestica descifrar cada contraseña:

contraseña	1 segundo	My C4ntrasEña	19 minutos
Contraseña	1 segundo	FuErtecontr@sEÑa	13 días
contraseña1	2 segundos	Es74ezmiCOntraSeña	8 años
contraseña17	3 minutos	Una_FuErte c@ntraSEña	33 años
Contraseña2017	3 minutos	Cr34rUnaFuErtec@ntraSEña	400 años

Consejos para Generar una Contraseña Fuerte

- Las contraseñas deben tener al menos ocho caracteres e incluir una combinación de letras, números y símbolos. Como regla general, cuanto más larga sea la contraseña, más fuerte es.
- Alternar entre mayúsculas y minúsculas ayuda a reforzar la contraseña. Por ejemplo, la palabra 'transferencia' podría escribirse 'tRAnsFeRenCIa'.
- Utilice "lenguaje hacker" sustituyendo algunas letras por números de aspecto similar o caracteres especiales. Por ejemplo, la palabra "banking" podría escribirse como "b@ Nk1nG".
- Basar su contraseña en una frase puede ayudarle a recordar combinaciones más complejas. Por ejemplo 'HumPty dUmpty S@T'.
- Otra buena manera de recordar una contraseña más compleja es pensar en una oración y luego utilizar la primera letra de cada palabra. Por ejemplo, 'Boston está a 4 horas de Nueva York en auto' podría ser tipiado 'Be@4hdNYea'.

Errores Comunes que Deben Evitarse

- No utilice información personal, palabras comunes, nombres, equipos deportivos o lugares en sus contraseñas.
- Agregar dígito numérico al final de una palabra conocida (por ejemplo, 'computadora1') no la convierte en una contraseña más segura.
- No reutilice la misma contraseña para diferentes cuentas online, ya que una única violación podría resultar en múltiples estafas.
- Nunca anote sus contraseñas; pueden ser robadas fácilmente de su computadora o escritorio.
- No comparta sus contraseñas con amigos, colegas o cualquier persona que solicite esta información por teléfono.

1581912 07/17