CONTRASEÑAS, ERRORES Y RECOMENDACIONES A LA HORA DE SU CREACIÓN

José Luis Romero González
Ingeniero de Sistemas
Especialista en Seguridad Informática
Profesor
Tecnológica FITEC
joselromero737@fitecvirtual.edu.co
Colombia

Mario Sorzano Serrano
Ingeniero de Sistemas
Profesor
Tecnológica FITEC
mariosorzano739@fitecvirtual.edu.co
Colombia

RESUMEN. En este documento se realiza un análisis de los problemas, que tienen los usuarios a la hora de crear sus contraseñas en las diferentes páginas que manejamos en Internet; los cuales resultan ser más comunes que lo que uno puede creer. El desconocimiento del buen manejo de las contraseñas o la pereza mental de algunos para recordar las diferentes contraseñas creadas, llevan a que los usuarios a realizar contraseñas nada seguras que le dejan la puerta abierta a los ciber-delincuentes. Por esta razón, crear una clave de acceso realmente fuerte se transforma en una tarea imprescindible para cualquier persona. Muchos usuarios piensan firmemente que ellos "nunca serán víctimas de ciber-delincuentes" por lo que cometen errores al crear sus contraseñas, que nunca deberían cometer y que constituyen un listado con las cosas que primero hacen los hackers para descubrirlas.

Palabras claves: contraseñas*, caracteres especiales, Internet, recomendaciones, seguridad informática, hacker, información, redes sociales, encriptación.*

ABSTRACT. In this article we are going to analyze the problems of the users that have when creating their passwords on different websites that handle; which they happen to be more common than we might believe. The ignorance of good management of passwords or mental laziness of some to remember different passwords than we created, users carries to perform any passwords that let you open the door to cyber - criminals. For this reason, creating a really strong access key becomes an essential task for anyone. Many users strongly believe that they “will never be victims of cyber-criminals “so they make mistakes when creating your own password, which should never make and constitute a list of the things that first make hackers to discover

Keywords: *passwords, special characters, Internet, recommendations, computer security, hacker, information, social networks, encryption.*

INTRODUCCIÓN

En un mundo que cada día es más avanzado en tecnología, y en el que cada vez más dejamos nuestra información en ella, las contraseñas juegan un papel importante para poderlas mantener protegidas de aquellas personas que puedan sustraer o alterar nuestros datos para el bien de ellos. La importancia de tener contraseñas seguras y su elección acertada es uno de los temas más importantes en seguridad informática, ya que de ellas depende la privacidad del usuario. Desde las redes sociales al correo electrónico o a las tarjetas y cuentas bancarias. Prueba de esta preocupación está en que empresas como Facebook está probando en EE.UU. un servicio de claves de acceso temporales que permite acceder a la red social en equipos públicos o a través de conexiones compartidas con total seguridad, mediante claves con una validez de 20 minutos que se envían al móvil del usuario que la solicita.
Pero muchos piensan que las contraseñas son el mecanismo de seguridad informática más confiable en nuestros días, Pero hay métodos más confiables ya que nuestras contraseñas están relacionadas con algunos datos de fácil acceso para personas externas como por ejemplo (cédula de ciudadanía, número de celulares o fechas especiales).

1. PROBLEMAS EN LA CREACIÓN DE LAS CONTRASEÑAS

En un mundo que cada día es más avanzado en tecnología, y en el que cada vez más dejamos nuestra información a disposición de esta, las contraseñas juegan un papel importante para poderlas mantener protegidas de aquellas personas que puedan sustraer o alterar nuestros datos para el bien de ellos.
Muchos piensan que las contraseñas son el mecanismo de seguridad informática más confiable en nuestros días, Pero hay métodos más confiables ya que nuestras contraseñas están relacionadas con algunos datos de fácil acceso para personas externas como por ejemplo (cédula de ciudadanía, número de celulares o fechas especiales).

El principal problema de las contraseñas es la mala concentración de los usuarios para recordarlas, y debido a esto los clientes suelen usar la misma contraseña para todos los tipos de cuentas que tienen ya sean correos o cuentas aún más importantes como las bancarias. Además, debemos

sumarle que esa contraseña suele ser, como se mencionó antes, datos de la vida cotidiana y de fácil acceso.
A medida que nos vamos acoplando a la evolución de las tecnologías, nos hemos acostumbrado a pensar en contraseñas más seguras que el típico "123456", o el nombre de nuestra mascota, mamá o papá, etc…
El problema radica en que muy seguramente ya ni estos nuevos códigos van a ser lo suficientemente seguros. Los propios métodos que se utiliza para dificultar el trabajo a los ciber-delincuentes son lo que, de manera irónica, facilitan más su tarea de descubrir nuestras contraseñas.

Muchas veces pensamos que nuestra contraseña es segura pero como sabemos que nuestra contraseña realmente no es una contraseña débil (weak) las contraseñas se filtran desde ataques informáticos a los servicios que las albergan. Para esto lo único que podemos hacer aparte de activar la doble verificación. Algunos de los errores más comunes son:

- Un carácter en mayúsculas, seguido de cinco en minúsculas y dos dígitos. Por ejemplo, Dulith57.
- Un carácter en mayúsculas, seguido de seis en minúsculas y dos dígitos. Por ejemplo, Abugmar64
- Un carácter en mayúsculas, seguido de tres en minúsculas y cuatro dígitos. Por ejemplo, Itio1981

Estos patrones son demasiados repetitivos en la mayoría de las contraseñas, permitiendo el fácil acceso a intrusos que deseen nuestra información.

Otros patrones que utilizamos para la creación de contraseñas son, empezar la contraseña con mayúsculas seguida de todo en minúsculas; añadir una o dos letras a una palabra demasiada corta para hacer de contraseña; añadir los números solo antes o después de las letras; Cuando la contraseña solicita un carácter especial, utilizar un símbolo de exclamación al final de la palabra;

Estos patrones se basan en la comodidad que buscamos a la hora de tener que recordar una contraseña, pero estos no son los únicos ya que cada vez la selección de contraseñas ha llegado a un punto en donde la pereza o muchas veces la necesidad de crear la contraseña de rapidez nos hace realizar errores mucho peores que los anteriores como por ejemplo, el no utilizar dos caracteres especiales o más en la contraseña, el utilizar códigos numéricos con secuencias ascendentes o descendentes (1234 o 4321), números duplicados (2222) o patrones creados por el teclado y que se pueden identificar fácilmente (como 2580 o 14789), utilizar palabras sencillas que están en diccionarios, que se pueden descubrir fácilmente con los programas más comunes para “hackear” cuentas, usar las palabras "Password" y “Admin” son graciosas, pero suelen ser las primeras que intentan los delincuentes al intentar penetrar a la cuenta, como también el colocar de contraseña lo mismo que usamos como nombre de usuario.

Un error muy común entre los ingenieros que manejan distintos dispositivos de red es la de no cambiar las contraseñas que vienen por defecto es estos dispositivos, el problema radica en que esas contraseñas son de conocimiento público, ya que buscando el manual de usuario de los dispositivos encontraremos la clave de acceso tales como los mencionados anteriormente o uno de los más comunes que traen los dispositivos que es la de ADMIN.

2. RECOMENDACIONES A LA HORA DE CREAR LAS CONTRASEÑAS

Existen páginas especializadas que se encargan de probar que tan segura son nuestras contraseñas como, por ejemplo, password strength checker o How secure is my password, en ellas podemos probar distintas contraseñas, seleccionar la más segura de todas y mirar que tan fuerte es mi contraseña actual y como la puedo mejorar

Pero para esto primero debes saber cómo crear una buena contraseña, ya vimos los errores más comunes, ahora veremos algunas recomendaciones para la creación.

La recomendación más importante que una persona debe tener en cuenta es que no involucre en la contraseña nada que tenga que ver con algún dato personal importantes, como numero de cedula de ciudadanía, fechas de cumpleaños, nuestros nombres o los nombres de algún ser querido.

Algunos trucos que se pueden tener en cuenta son

2.1. FORMACIÓN DE PALABRAS NUEVAS EN BASE A PALABRAS EXISTENTES

Escoger dos palabras para forma una palabra nueva, es un método muy común a la hora de la creación de nuevas contraseñas, es un método sencillo, pero que genera problemas a la hora de la memorización.

El método es el siguiente

Seleccionamos las dos palabras, pueden ser palabras que no tienen nada que ver o un nombre compuesto, lo ideal es que sean palabras largas, por ejemplo, Jorge Enrique. Luego separamos las letras y las mezclamos hasta forma una nueva palabra, no necesariamente la nueva palabra puede significar algo, en muchos casos parecen letras al azar sin ningún sentido.

Luis Enrique = lierqeusniu

2.2. MEZCLAR PALABRAS CON NÚMEROS

Aunque anteriormente decíamos que mezclar letras con números era uno de los patrones más rápidos de descifrar contraseñas, si mezclamos las palabras y los números de manera adecuada, podemos crear una contraseña bastante fuerte.

Tomemos por ejemplo la palabra flash y los números 9708. La idea no es solo colocar la palabra y los numero si no mezclarlos de forma de colocar palabras que no tengan sentido

FLASH 9708 = F9L7A0S8H

2.3 MEZCLAR PALABRAS O CARACTERES

para realizar este forma de método de seguridad usted como usuario necesita que dicha contraseña que usted como cliente considere confiable por ejemplo escogeremos el anterior “ejemplo en el punto 2.2” con la contraseña FLASH9708, para obtener dicha seguridad usted como cliente debe agregarle una combinación de caracteres como “#$%&” o mejor aún, si quiere más confidencialidad a su contraseña le puede agregar la letra Ñ, ya que esta letra no se encuentra en el abecedario norteamericano. ejemplo FLASH 9708Ñ

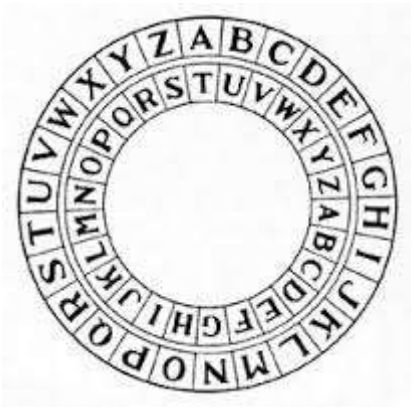
2.4 ENCRIPTACIÓN

La encriptación es la solución para tener más segura toda la información que tenemos, ya que esta sirve para enmascarar los datos, con el objetivo de que sean incomprensibles para cualquier agente no autorizado

También hay que tener en cuenta el evitar palabras o frases lógicas en las contraseñas, empezar con una letra mayúscula, o repetir siempre el mismo tipo de carácter especial. Hay que tener en cuenta que el reciclaje de contraseñas tampoco es recomendable.

2.5 CIPHER WHEEL

La rueda de cifrado es una técnica que data de los años 1743 cuando el señor Thomas Jefferson creó un aparato que consistía en girar unos cilindro que tenían el abecedario cuando se posicionan todos de una forma correcta se abría la caja que contenía algún secreto, como lo muestra en el dibujo para poder encriptar información,



2.6 SOFTWARE Y APLICACIONES DE CIFRADO

una de las formas más rápidas para proteger la seguridad de sus datos es utilizando softwares confiables como el de “MEO File Encryption Software” que sirve para Windows y Mac, una herramienta muy confiable para los que queremos proteger nuestra información, y aunque hay muchas software es una de las más confiables en el mercado, hoy por hoy empresas como La industria informática GOOGLE ha

reaccionado con preocupación a las filtraciones del ex técnico de la CIA, Edward Snowden decidieron acelerar el proceso de encriptación para mejorar su confiabilidad en los usuarios.

La criptografía asimétrica utiliza dos claves distintas, pero que matemáticamente son equivalentes. Así, la información que es cifrada con una, puede ser descifrada con la otra. Sin embargo, el hecho de conocer la clave pública no revela la clave privada.

Para proveer integridad, se calcula un valor único (hash) para el mensaje utilizando algún algoritmo de digestión (md5, sha1, etc.). Para proveer autenticidad, se cifra ese valor con clave privada del emisor, la cual se agrega al final del mensaje enviado, junto con el nombre del algoritmo utilizado.

Utilizando todas estas técnicas de encriptación usted como usuario va a tener un conocimiento un poco más avanzado lo que es acerca de las contraseñas y como usted podrá defenderse de una manera sencilla pero eficaz en contra de las personas que quieren infiltrarse en sus cuentas.

Esperamos que este artículo haya sido de su ayuda y de su agrado, pero más que eso que haya sido de su ayuda profesional en el conocimiento de las nuevas tecnologías y sus complejos.