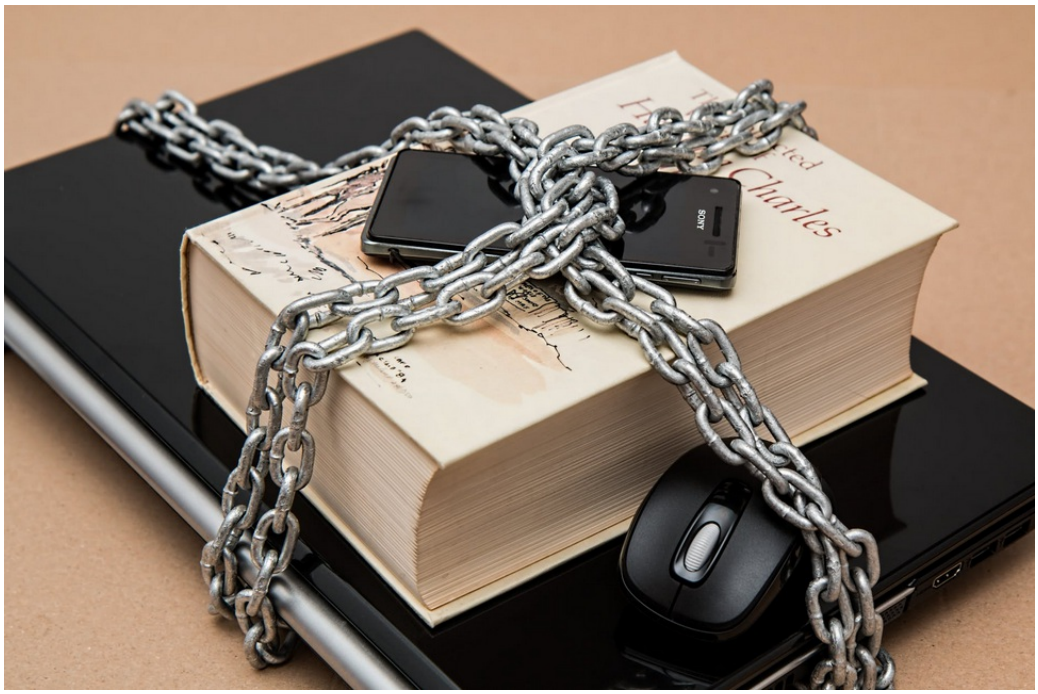
Mantén tus contraseñas seguras

Publicado el El Informatico - 30 de agosto de 2021 -



Si eres de esas personas que usan la misma contraseña para todo, o usas contraseñas con nombres, fechas, o palabras que aparezcan en algún diccionario de cualquier lengua, entonces deberías echarle un ojo a éste artículo. Uno de los mayores vectores de ataque en internet es el uso de contraseñas no seguras. ¿Cómo sería entonces la contraseña perfecta?

Tus contraseñas deberían contener al menos 12 caracteres.

En algunos sitios se especifica que deben ser un mínimo ocho caracteres, pero creo yo que con el hardware del que disponemos ahora es mejor usar una cantidad mayor para estar seguros. Cuanto mayor sea el número de caracteres, mayor será la resistencia a ataques de fuerza bruta. Aunque por supuesto, hay otros factores a tener en cuenta.

Las contraseñas deben tener todo tipo de caracteres.

Para incrementar la seguridad frente a ataques de fuerza bruta, diccionario, o simple

deducción, es mejor usar mezclas de caracteres de modo que la contraseña parezca aleatoria y no tenga sentido. Debemos usar letras (tanto mayúsculas como minúsculas), números, símbolos y signos de puntuación, mezclados de forma que parezca aleatoria.

Hay gente que aconseja usar símbolos en lugar de letras (Llamado "13375p34k"), usar iniciales y dígitos de fechas mezclados con algún símbolo aleatorio. Yo no recomiendo eso. En su lugar, recomiendo generar contraseñas aleatorias que sean lo suficientemente fuertes.

No uses palabras, fechas, nombres, etc.

Son muy fáciles de adivinar y a veces los atacantes usan diccionarios con contraseñas comunes que usa todo el mundo. Puedes pensar que usando la fecha en la que encontraste al amor de tu vida mezclado con el nombre de tu perro tu cuenta estará segura, pero te aseguro que no es así.

Tus contraseñas deben ser únicas.

Memorizar contraseñas da palo, por eso mucha gente usa la misma contraseña para todo. Para el correo, para la cuenta de paypal, y para acceder al foro de manolito.com.

Ahora imagínate que el foro de manolito sufre un robo de datos y un atacante consiguiera hacerse con las contraseñas que hay en la base de datos. ¿Qué crees que va a pasar con tu cuenta de correo, tu cuenta de paypal, y todas las cuentas asociadas a tu correo electrónico?

No uses la misma contraseña para todo. Si no puedes memorizarlas todas, al menos usa un gestor de contraseñas como KeePass.

La contraseña debe cambiar periódicamente.

A veces los servicios sufren brechas de seguridad en sus bases de datos. Normalmente las contraseñas están encriptadas (o así debería de ser), pero eso no impide que un atacante pueda romper la encriptación con el tiempo. Si la encriptación es buena, el atacante puede tardar meses o incluso años en romperla. Tiempo más que suficiente para poder cambiar la contraseña.

Debes cambiar la contraseña al menos una vez al mes. Por lo menos de los servicios más importantes.

Memoriza las contraseñas, o usa un gestor de contraseñas.

Evidentemente, si anotamos las contraseñas en un post-it o en un cuaderno (o en un

archivo de texto en nuestro dispositivo, sobre todo si es un móvil o un portátil), cualquiera podría hacerse con ellas simplemente mirando en donde las tengas apuntadas.

Lo más seguro es mantener las contraseñas en nuestra cabeza. Pero seamos sensatos, usamos decenas de contraseñas en internet y es casi imposible memorizarlas todas, más teniendo en cuenta lo mencionado anteriormente. En estos casos, lo mejor es usar un gestor de contraseñas como Keepass.

De éste modo, tendremos todas las contraseñas en un archivo encriptado, teniendo que memorizar sólo una contraseña para acceder a éste archivo (y mejor que esta sea fuerte).

Naturalmente, si tenemos todas nuestras contraseñas en un único archivo, en caso de robo de éstos datos un atacante podría hacerse con las contraseñas. No obstante, si la contraseña es lo suficientemente fuerte y usamos un número elevado de iteraciones para la generación de las claves de la base de datos de *keepass* (aunque tarde un tiempo en abrir el archivo, mejor eso que ser un blanco fácil), tendremos tiempo de sobra para cambiar las contraseñas antes de que el atacante se haga con ellas.

Por eso, lo más seguro es tenerlas en la cabeza. Aún no se ha conseguido acceder a nuestra cabeza, así que ahí están seguras mientras no se las digas a nadie.

NUNCA le digas a nadie tu contraseña.

Nunca, y bajo ningún concepto, debes darle a NADIE ninguna de tus contraseñas. Los administradores y operadores de los distintos servicios que usas en internet deben tener acceso directo a la base de datos, por lo que nadie necesita tu contraseña. Y aun en el caso de que realmente un administrador u operador relacionado con el servicio te la pidiera, no debes darla. Búscate un servicio mejor donde tengan un sistema en condiciones.

Aunque pienses que tu contraseña es aleatoria y única, tú nunca sabes qué tipo de información podría obtener un atacante sobre tus contraseñas. Hay gente muy inteligente capaz de extraer información incluso de las contraseñas más fuertes, pudiendo incluso llegar a averiguar el resto de tus contraseñas.

Ejemplos de contraseñas no seguras:

- **12345**: ¿Cuánto crees que van a tardar en adivinar ésta secuencia numérica? Ni dos segundos.
- **9427**: ¿Es éste el pin de tu teléfono? Creo que incluso 12345 sería más seguro. ¡No hagas ésto!
- **pepe21**: Contiene menos de 12 caracteres, usa sólo minúsculas y números, y encima contiene un nombre y los últimos dígitos de un año. Fácil de adivinar,

incluso por fuerza bruta o con un ataque de diccionario.

- **raquelxpepe51209**: Tiene más de 12 caracteres pero contiene nombres y una fecha. Fácil de averiguar con un ataque de diccionario, sobre todo si conocen a las víctimas.
- **9427pepe21**: Una mezcla del PIN del teléfono de Pepe, su nombre (en minúsculas), y los dos últimos dígitos del año de inscripción en el servicio. Todo fácil de averiguar. ¡No mezcles contraseñas!
- **DaRkLoRd93**: Muy chula, pero también muy fácil de averiguar usando ataques de fuerza bruta o diccionario. Sobre todo si "DaRkLoRd" es tu nickname.

Ejemplo de contraseñas seguras (no uses éstas, son solo ejemplos):

- **Ii.Zfu$HAuQN_3Bfmb!E**: 20 caracteres, usa una combinación de todo tipo de caracteres de forma completamente aleatoria, y no contiene palabras ni nombres ni fechas. Imposible de adivinar y muy difícil de obtener mediante fuerza bruta (Dependiendo de la encriptación usada podría llevar muchos años averiguarla).
- **)M6vR0g"xJ2^**: Sólo son doce caracteres, pero combina todo tipo de caracteres de forma aleatoria. Al igual que antes, es imposible de adivinar y muy difícil de obtener mediante cualquier tipo de ataque básico. Al ser sólo doce caracteres es menos segura que la anterior, pero igualmente le dará mucho trabajo a cualquier atacante.

Para sysadmins: Nunca almacenes las contraseñas en texto plano.

Las contraseñas deben estar siempre encriptadas. Es más, deben ir encriptadas **desde el cliente al servidor**, usando algún algoritmo de un solo paso. Este algoritmo debe ser criptográficamente seguro, es decir, no vale usar MD5. Por ejemplo, PHP incluye la función pasword_hash(), que permite encriptar la contraseña de manera segura. Node (javaScript) incluye librerías como Bcrypt para éste propósito. **En ningún caso es justificable el uso de contraseñas en texto plano**.

Sigue la normativa GDPR.

Debes especificar donde se almacenan los datos de los usuarios (incluyendo las contraseñas, por supuesto), quien es el responsable de custodiar esos datos, cómo y donde están esos datos, así como el protocolo de actuación en caso de sufrir un filtrado de datos.

Si sufres una filtración de los datos de tus usuarios, debes informarles inmediatamente de ello, así como sugerirles un cambio de la contraseña. De no hacerlo, podrías ser sancionado con una buena multa en función del daño.

ANTERIOR

Obtén información meteorológica con Python

SIGUIENTE

Protégete ante el Ransomware

Buscar ...

Entradas Recientes

- El Metaverso: Nada nuevo en el horizonte
- Estafas telefónicas: ¡No caigas en la trampa!
- Jueves de buenas noticias
- Facebook, una vez más, en problemas. Y es su propia culpa.
- Si usas Twitch, cambia tu contraseña de inmediato
- Diferencias entre Internet y La Web. ¿Qué es cada uno?

Categorías

Actualidad Android Básicos Ciberseguridad Criptografía Emulación / Virtualización FOSS Hacking Informática Internet Juegos Opinion Otros Personal Privacidad Programación Tecnología Time Machine Tutoriales

RSS

Subscribirse al feed RSS