

Seguridad en sus Cuentas

En [Hostdime](#) Nos preocupamos por la seguridad en las cuentas de nuestros Clientes, es por eso que a continuación indicaremos una serie de tips de seguridad que le ayudara a tener unas cuentas Mucho mas seguras y con menos problemas de seguridad

1) Usar Ingresos por separado para todas las BD's (Crear usuarios para las BD's) con cada una de ellas con una contraseña única, distinta de la del inicio de sesión del cpanel principal.

Este es un método muy popular para recabar las contraseñas (porque todas las conexiones a las bases de datos requieren de información de acceso a las mismas. Si usted usa su nombre de usuario cpanel y le roban la contraseña, les estará dando libre acceso a toda su cuenta.

2) No guarde su contraseña de la cuenta en texto plano!!!. Esto es muy importante. No hay necesidad de hacerlo.

En ninguna circunstancia, almacene la información de acceso al cpanel en un archivo de texto.

3) Siempre utilice los permisos adecuados: si un archivo o un directorio no tiene que ser modificada por el servidor web, no es necesario que todo el mundo pueda escribir en él. Modificar los permisos pueden resultar tedioso, pero no se sienta tentado a simplemente hacer todos sus archivos 777. Esto sólo conducirá a más dolores de cabeza más adelante.

4) Manténgase al corriente de sus scripts PHP: A menudo instalamos script's sólo para probarlo, jugamos con él durante un tiempo, y luego nos olvidamos que sigue en el servidor. Este es un riesgo de seguridad importante, Si usted no va a utilizar una determinada pieza de software, es mejor eliminarlo. Si instala software de terceros, suscribase a las listas de correo del proveedor, para que lo mantenga al tanto

de busg's o actualizaciones, para que siempre tenga actualizado y seguro su sistema y su servidor.

5) Mantenga siempre una contraseña segura: Las contraseñas deben tener 6-8 caracteres alfanuméricos y también asegurarse de que no es una palabra común. Un truco que se recomienda es usar una frase, y hacer que su contraseña la primera letra de la frase. Por ejemplo, si la frase es "My [website](#) is so cool, I can make a million dollars with it!", A continuación, su contraseña sería "MwiscIcmamdwi!". Por supuesto, la contraseña puede ser un poco fea, pero recordando que es bastante fácil, ya que es una expresión natural, se encuentra que la contraseña se convierte en una parte de su memoria y no hay más necesidad de explicar la frase.

6) También deben asegurarse de que los sistemas y equipos utilizados para administrar las cuentas estén libres de troyanos / malware. Malware es comúnmente usado para comprometer contraseñas en casos como este.

Le desaconsejamos:

No utilice información personal (nombres, apellidos, fecha de nacimiento, número de DNI, número de su celular o teléfono) ni de las personas de su alrededor.

No use palabras del diccionario.

No ponga el usuario como su contraseña, tampoco secuencias de números como 123456 o 2222 y mucho menos la palabra password o contraseña como la contraseña de su cuenta.

No use la misma contraseña para todas sus cuentas (es decir no use la misma contraseña para sus correos, redes sociales, sus [cuentas de hosting](#), panel de dominios, etc.)

No le de su contraseña a nadie.

No teclee sus contraseñas en ordenadores en los que usted no controle la seguridad del mismo, como pueden ser en cabinas de Internet, cibercafés, en wifis abiertas en lugares públicos; ya que esas redes pueden estar siendo monitoreadas por intrusos.