Cómo proteger tu información y no morir en el intento

HostDime quiere darte los siguientes consejos que puedes poder en práctica **para que protejas tu información y evites pérdida o accesos no deseados.**

En su mayoría, **todo tipo de abuso** [SPAM, Phishing, Hackeo, Accesos no permitidos] **están asociados a compromisos en las contraseñas**, el nivel de seguridad que posea la misma y los equipos en donde haces conexión.

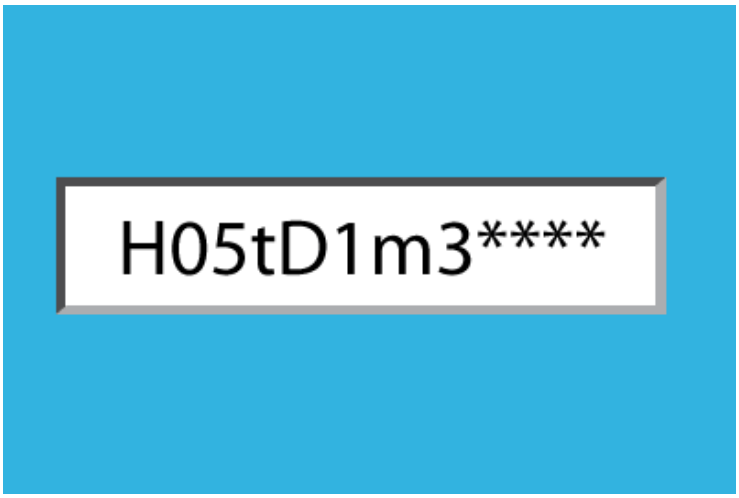
A continuación te damos algunos tips que puedes poner en práctica para asegurar tus contraseñas y así reduces las posibilidades de un abuso o compromiso.

1. Cambia periódicamente tus contraseñas

El uso de una misma contraseña durante largos períodos de tiempo te hace vulnerable a ataques de fuerza bruta que busquen identificar tu contraseña actual. **Al no cambiarla periódicamente, estas permitiendo que sea más fácil descifrarla ya que dispone de más tiempo para ello.**

Por tanto te aconsejamos cambies tus contraseñas de acceso [correo, acceso panel de control, acceso portal de cliente, FTP, acceso root o cualquier tipo de contraseña que dispongas] **con una periodicidad entre 1 a 3 meses.**

2. Asigna contraseñas seguras



La seguridad de una contraseña igualmente se encuentra asociada a la **longitud y caracteres** que utilices. Aconsejamos asignes contraseñas que contenga núm3r05, letras MAYÚSCULAS y minúsculas, C@r@cteres especiales con una longitud mínima de 10 dígitos. La combinación de estos 4 signos permitirán un nivel de seguridad muy alto que evitará que ataques de fuerza bruta sean eficientes.

Igualmente puedes utilizar los generadores de contraseña que te suministre el panel de control, estos generadores están configurados para siempre suministrarse contraseñas de alto nivel de seguridad.

3. Escanea tus equipos periódicamente

Mantener tus equipos/dispositivos libres de cualquier tipo de Malware/Trojano evitará en un muy alto porcentaje cualquier tipo de vulnerabilidad. Muchos virus están diseñados para **robar contraseñas e inyectar código malicioso, comprometer contraseñas y enviar SPAM o robo de información** entre otros.

Tu equipo debe estar libre de cualquier tipo de Malware para que tu información y tus operaciones sean seguras.Asegura tu equipo con un Antivirus conocido por su eficacia y **programa escaneos en cortos periodos de tiempo**. Igualmente un consejo adicional es que **pruebes con más de un Antivirus el escaneo de tu servidor.**

4. Guarda muy bien tus contraseñas

Evita dejar vulnerables tus contraseñas en cualquier lugar. Si llevas tus contraseñas contigo o guardas tus contraseñas en archivos de texto, evita dejarlas al acceso general. Tus contraseñas son sólo para ti o para quienes deban tener acceso a ella. Una contraseña no debe ser pública a menos que realmente lo requieras, y aunque un número indefinido de personas la usen, **debes aplicar protocolos adicionales** para evitar que personal que no deba tener acceso pueda verla o utilizarla.

Ver también: La Verificación En Dos Pasos Google (2-Step Verification), Seguridad en sus Cuentas, La Seguridad en HostDime es Importante