



Claves, claves, claves y más claves!

Es increíble la cantidad de claves que tenemos que crear, memorizar y utilizar debido al incremento en la seguridad y los servicios digitales. Ahora tenemos que manejar claves en el celular para bloquearlo (cosa que no sirve de mucho, triste pero cierto), en las tarjetas para usar cajeros automáticos, para abrir puertas, para cajas fuertes, para iniciar computadoras, para abrir sistemas, para buzones de correo, para servicios bancarios, para tiendas en línea y si nos va bien, allí nos quedamos.

Me considero un poco paranoico así que generalmente cambio con frecuencia mis contraseñas y no las repito a través de servicios, a diferencia del clásico usuario que he encontrado muchas veces diciéndome "Mi contraseña es pepe, es la que uso siempre". Sonará divertido pero es real. Y aún más divertido y peligroso es aquel que dice "Mi clave es 1050, es la que uso para todo, hasta para mis tarjetas". No es broma, es más común de lo que piensas.

Así que en vista de la gran cantidad de claves que debemos proteger, allí te van algunos consejos para proteger mejor tu intimidad, tus datos y hasta tu dinero.

1. La regla de oro: no compartas con nadie tus contraseñas personales, obviamente quedan fuera de esta regla las contraseñas relacionadas con tu trabajo, las que generalmente serán conocidas por el personal de IT de tu empresa, así que no utilices las mismas para tus servicios personales y para tus servicios laborales. Una encuesta reciente de Infosecurity Europe reveló que el 45% de las mujeres (sin ánimo de sonar machista) y el 10% de los hombres darían su contraseña ¡a cambio de un chocolate!
2. Si quieres repetir contraseñas (no recomendable), define al menos 3 diferentes y úsalas donde sean aceptadas, en el siguiente orden de preferencia:

Una con signos, números, letras en mayúsculas y minúsculas
Estas son las más seguras ya que son muy difíciles de descifrar, incluso al ser atacadas con software especial ya que la cantidad de combinaciones de caracteres es increíblemente grande. Por ejemplo, si tu contraseña fuera MiClave50\$ y alguien con un programa automático inicia un ataque probando todas las combinaciones posibles, serían necesarios más de 3 años con la computadora trabajando las 24 horas, para poder encontrar la clave. ¿Tendrá alguien tanta paciencia? Una buena práctica para recordarlas es cambiar letras por símbolos, por ejemplo, escribes clave cambiando la letra "l" por "!", o escribes \$creto, cambiando la "s" por "\$".

Una con mayúsculas y minúsculas
No utilices claves cortas, y de preferencia mezcla mayúsculas y minúsculas.
No utilices datos tan predecibles como tu nombre, apellido o sobrenombre o los de tu pareja ya que son las primeras claves que probaría cualquier persona.

Una con números

No utilices tu fecha de cumpleaños, aniversario, dirección etc. De preferencia selecciona el mayor número aceptado al azar y memorízalo. Después de todo, dicen que basta con repetir algo 21 veces para aprenderlo.

3. No anotes tus contraseñas en cualquier parte, a veces es necesario anotarlas pero no las dejes a la vista y de preferencia no seas tan descriptivo (a) a la hora de hacerlo, así que no escribas "Clave para el Banco XX: MiClave50\$".
4. En lo posible, no entres a tus cuentas de correo, servicios bancarios o cuentas de tiendas en línea en cualquier computadora, esto por supuesto incluye los famosos café Internet. Muchas computadoras pueden tener instalados intencionalmente o no, programas que graban toda actividad de forma transparente al usuario así que alguien podría obtener tus contraseñas fácilmente. Si fuera muy necesario hacerlo, cambia cuanto antes tu contraseña en alguna computadora que sea de tu confianza.
5. Mantén protegida y actualizada tu computadora. Ya no es suficiente con tener un antivirus, así que te recomiendo además tener un anti-spyware residente en memoria y al menos otro no residente para escanear periódicamente. En otro artículo te recomendaré que software puedes utilizar para esto.
6. No descargues cualquier software de Internet, aún cuando parezca genuino, inocente o útil. Un ejemplo de esto es G-Archiver, un programa para hacer backup de tus correos de Gmail. Recientemente se descubrió que cuando lo utilizas, tu usuario y contraseña son enviadas por correo a su creador!

Disfruta de esta era de tecnología, cada día aparece algo nuevo e impresionante pero recuerda que ante todo, debes ser muy analítico y un poco desconfiado. Si vas a utilizar un servicio, busca antes en Internet que comentarios se hacen, las experiencias buenas o malas de otros usuarios pueden ser un buen punto de partida para tomar una decisión.

Publicado por Alfredo Rivera

Blog de Mundo en Línea
-- Un vistazo al mundo de la tecnología --
<http://www.blog.mundoenlinea.net>