Lo seguro es tratar de no repetir contraseñas, debido especialmente a que cada sitio web puede tener diferentes niveles de vulnerabilidad de cara a que éstas sean hechas públicas y también por el simple hecho de la peligrosidad que existe en tener una llave que abra todas las puertas.

Por eso, la pregunta de varios expertos es cómo llegar a la contraseña perfecta. Hay varias opciones, según puede leerse en Livescience: un inicio de sesión universal para todos los servicios que empleemos, el uso del teléfono móvil para acceder a estos, passwords basados en características físicas de su dueño, tales como patrones del iris del ojo o la voz.

Para ser eficaz, hoy en día se nos piden dos cosas principalmente: por un lado, contraseñas que mezclen todo tipo de caracteres, y por otro, que esa clave sea modificada cada poco tiempo. De igual manera, se suelen estudiar las contraseñas más empleadas, a la vez que se ofrecen recomendaciones y generadores de éstas, para los menos creativos. El problema es que lo que nos hace más fuertes (contraseñas distintas para cada servicio) también se vuelve nuestro punto débil (recordarlas todas puede llegar a ser imposible).

UN ÚNICO INICIO DE SESIÓN

Alrededor de nueve millones de sitios web aceptan ya un inicio de sesión único llamado OpenID. Este tipo de acceso descentralizado es apoyado desde grandes de Internet como Google, Yahoo! y la red social Facebook.

"El usuario se autentica con un sólo proveedor, evitando la dispersión actual en Internet", explica Brian Kissel, CEO de JanRain y presidente de la Fundación OpenID.

Existen críticos con este tipo de inicio de sesión, que argumentan que si un sitio es más vulnerable a un ataque puede provocar que la contraseña 'universal' caiga en manos de otras personas.

CON EL TELÉFONO MÓVIL

Bob Bakley, del grupo de investigación Burton, ve el futuro de las contraseñas muy cerca de los móviles. Piensa que el inicio de sesión único se hará a través del teléfono móvil.

"Los móviles podrían actuar como claves para entrar en nuestro ordenador y a los servicios a los que nos conectemos, sin necesidad de otras contraseñas adicionales", explicaba Bakley a TechNewsDaily recientemente, a la vez que añadía que el mismo dispositivo móvil detectaría si alguien ha accedido a nuestra clave.

CONTRASEÑAS BIOMÉTRICA

A través de características físicas propias del individuo, tales como rasgos del iris, huellas dactilares, patrones de voz...

Sus promotores la defienden del resto propuestas asegurando que su índice de error no supera el 1% en ningún caso (el reconocimiento de huellas dactilares en un portátil, por ejemplo), algo de lo que se aprovechan sus detractores, quienes argumentan que la identificación biométrica no es nunca una identificación 100% personal. También señalan que las condiciones que rodean (ambientales o de salud) al sujeto puede ofrecer problemas en este campo.

Fuente: *www.madrimasd.org*