¿Cómo sobrevivir a los ataques a empresas que filtran contraseñas?

domingo, 29 de julio de 2012

En realidad el usuario no puede hacer nada para proteger sus datos frente a un ataque dirigido a sus proveedores de servicios, pero algunos consejos básicos pueden evitar grandes desastres si se comprometen sus contraseñas.
Cada vez son más frecuentes y nos referimos a los ataques a proveedores de servicios en Internet cuyo final es el filtrado de las contraseñas personales de sus usuarios. Sin ir más lejos, el pasado mes de junio se filtraron 6,46 millones de contraseñas de usuarios de LinkedIn. Poco después, a principios de julio, se descubrió que se habían filtrado 400 mil contraseñas de Yahoo Voices.

Tal y como afirma Dmitry Bestuzhev, Analista de Kaspersky Lab, en su blog: Estos no son casos aislados; hoy en día se pueden ver muchos ataques que provocan filtraciones de datos personales. Otro ejemplo es el filtrado de información personal de los usuarios de uno de los conocidos foros de Android y el ataque al foro de desarrolladores de NVIDIA. Hay que destacar que muchos de los ataques no se anuncian al público y la comunidad de Internet no tiene conocimiento de ellos.

Entonces, ¿qué hacemos cuando nuestras contraseñas pueden haberse filtrado? Por supuesto, el usuario no puede hacer nada para protegerse frente a un ataque dirigido a sus proveedores de servicios y evitar las filtraciones, pero estos son algunos consejos básicos para evitar grandes desastres si se comprometen contraseñas.

1. Utilice una contraseña diferente para cada recurso de Internet. No reutilice la misma contraseña para entrar a diferentes servicios. Si lo hace, pone en riesgo muchas de sus cuentas a la vez.

2. Utilice contraseñas complejas. Esto significa que deben tener una combinación de símbolos, letras y caracteres especiales.

3. A algunos usuarios les cuesta trabajo recordar las contraseñas complejas. En este caso, una buena solución sería utilizar un administrador de contraseñas de alguna solución de seguridad que las unifique y solo haya que recordar una en el dispositivo que utilicemos.

Recuerda que no puedes evitar que tu proveedor de servicios sufra un ataque, pero puedes evitar catástrofes si te aseguras de que no se comprometan todas tus cuentas al mismo tiempo porque usabas la misma contraseña.

Para acceder al blog: http://www.viruslist.com/sp/weblog?weblogid=208188651

Kaspersky Lab
Kaspersky Lab es una de las mayores compañías antivirus de Europa. Kaspersky Lab proporciona una de las protecciones más inmediatas del mundo contra amenazas a la seguridad informática, incluyendo virus, programas espía, fraudes cibernéticos, ataques de hacker, robo de información confidencial y correo spam. La compañía es uno de los cuatro principales fabricantes mundiales de soluciones de seguridad informática para usuarios finales. Los productos y soluciones de Kaspersky Lab proporcionan uno de los tiempos de respuesta más rápidos y de los niveles de detección más altos de la industria, tanto para usuarios particulares, pequeñas y medianas empresas y grandes corporaciones, como para el entorno informático móvil. La tecnología de Kaspersky® también se integra como parte de otros productos y servicios proveedores líderes soluciones informáticas de seguridad. Para obtener más información, visite www.kaspersky.es. Para obtener información más reciente sobre antivirus, antiespías, antispam y otras amenazas informáticas, además de las últimas tendencias, visite www.viruslist.es

Síganos en: http://twitter.com/#!/KasperskyES http://www.facebook.com/kasperskyes