

Verificá si tu cuenta de mail está comprometida

Se han identificado más de 12 archivos con 2.700 millones de registros que contienen direcciones de mail y contraseñas. Se trata de una de las brechas de seguridad más grandes en los últimos tiempos.

Al parecer, todo comenzó con filtraciones de archivos que estaban en foros de hackers. Un archivo compilando esta información, bautizado #Collection1 anduvo circulando por la nube. En este archivo había más de 140 millones de cuentas y 10 millones de contraseñas.

"La lista parecía estar diseñada para ser utilizada en los llamados ataques de relleno de credenciales, en los cuales los hackers tiran combinaciones de correo y contraseña en algún sitio o servicio determinado. Estos son procesos usualmente automatizados que se aprovechan especialmente de las personas que reutilizan las contraseñas en toda la web", detalla un experto en cibercrimen.

Cómo saber si tu correo puede ser vulnerado

Para verificar si tu correo estaba incluido en estas listas, abrí un navegador y dirigite a la página:

<https://haveibeenpwned.com/>

Cuál es la gravedad del problema

Es posible que los datos del usuario hayan llegado a la lista si, por ejemplo, se registró en un sitio y luego ese sitio fue hackeado. Así se obtuvieron las combinaciones de correo y contraseñas que se filtraron. Si el usuario usa la misma combinación de correo y password en la actualidad, entonces ese dato podría ser la puerta de entrada para que los hackers ingresen a sus correos, redes sociales o cualquier otra plataforma donde se utilicen esas credenciales expuestas.

Cómo protegerte

Si estás en la lista, primero deberías seguir estas reglas:

- Cambiar la clave de tu correo
- Cambiar la clave de cualquier otro servicio donde usaste la misma clave
- Utilizar el factor de doble autenticación en aquellos servicios que lo permitan

Como siempre, es importante tener el sistema operativo actualizado, contactar con una solución de seguridad y evitar descargar contenido de sitios poco fiables o aplicaciones de otros lugares que no sean las tiendas oficiales y evitar conectarse a redes wifi públicas.