

Cómo crear contraseñas seguras para proteger tus cuentas bancarias

Hoy en día, gran parte de nuestras operaciones financieras se realizan desde un celular o una computadora. Consultar el saldo, hacer transferencias, pagar servicios o invertir son actividades cotidianas que ofrecen comodidad, pero también requieren medidas de seguridad para proteger nuestro dinero.

Uno de los errores más comunes es utilizar contraseñas fáciles de adivinar o repetir la misma clave en varias cuentas. Aunque parezca una decisión sin importancia, una contraseña débil puede facilitar que los delincuentes accedan a información bancaria y cometan fraudes.

¿Por qué son tan importantes las contraseñas?

Las contraseñas funcionan como la primera barrera de protección para tus cuentas bancarias, aplicaciones financieras y servicios digitales.

Si una persona obtiene tu contraseña, puede consultar tu información personal, cambiar tus datos de acceso, ingresar a tu banca en línea y realizar transacciones, así como utilizar tu identidad para cometer fraudes.

Por eso, una contraseña fuerte es uno de los elementos más importantes para proteger tanto tu información como tu patrimonio.

¿Qué características debe tener una contraseña segura?

Una contraseña segura debe ser fácil de recordar para ti, pero difícil de adivinar para otras personas y para los programas automatizados que utilizan los ciberdelincuentes.

Para eso, se recomienda que la contraseña tenga los siguientes elementos:

- Al menos 12 caracteres (esto depende del número que cada servicio permita agregar).
- Letras mayúsculas y minúsculas.
- Números.
- Caracteres especiales (&\$?+).
- Una combinación aleatoria que no forme palabras comunes.

Mientras más larga y compleja sea la contraseña, mayor será su nivel de protección. Por eso, una alternativa segura consiste en utilizar frases que combinen palabras, números y símbolos, así como sustituir algunas letras por símbolos o números en las palabras, por ejemplo: "B0\$qu3", en lugar de "Bosque".

Evita utilizar información personal

Uno de los errores más frecuentes consiste en crear contraseñas con datos fáciles de obtener. Por eso, se recomienda no usar:

- Tu nombre, el de tu pareja, hijos o mascotas.
- Fecha de nacimiento.
- Número telefónico.
- Equipos deportivos, artistas o personajes favoritos.
- Secuencias como "123456", "abcdef" o "qwerty".

Este tipo de información puede encontrarse fácilmente en redes sociales o mediante ingeniería social.

No reutilices la misma contraseña

Puede parecer práctico utilizar la misma contraseña para todas tus cuentas, pero representa un riesgo importante.

Si un ciberdelincuente obtiene la contraseña de una plataforma, podría intentar utilizarla para acceder a tu banca móvil, correo electrónico, redes sociales, plataformas de compras y aplicaciones financieras.



bancodonde.com

Por eso, lo más recomendable es utilizar una contraseña distinta para cada servicio importante.

Activa la autenticación en dos pasos

La contraseña no debe ser la única medida de protección. Siempre que sea posible, activa la autenticación de dos factores.

Con esta función, además de la contraseña, será necesario confirmar el acceso mediante un código enviado al celular, una aplicación autenticadora o bien, a través de datos biométricos como huella digital o reconocimiento facial.

Así, aunque alguien conozca tu contraseña, le resultará mucho más difícil tener acceso a tu cuenta.

Utiliza un administrador de contraseñas

Recordar muchas contraseñas diferentes puede ser complicado y para evitar olvidos o confusiones entre ellas, lo más recomendable es usar administradores de contraseñas. Se trata de herramientas que permiten generar claves seguras, guardarlas de forma cifrada y autocompletar el acceso a diferentes servicios.

Solo necesitarás recordar una contraseña principal para acceder al resto de tus datos de acceso a diferentes plataformas y servicios. Eso sí, asegúrate de utilizar un administrador reconocido y mantener protegida la contraseña maestra.

Cambia tus contraseñas cuando exista algún riesgo

No es necesario cambiar todas tus contraseñas cada mes si son fuertes y no ha ocurrido ningún incidente.

Sin embargo, sí conviene actualizarlas cuando sospechas que alguien las conoce, si recibes una notificación de una filtración de datos, cuando detectas movimientos extraños en alguna cuenta o si compartiste accidentalmente tus datos de acceso.



bancodonde.com

En estos casos, cambia la contraseña inmediatamente y revisa la actividad reciente de la cuenta.

Como puedes ver, en un entorno cada vez más digital, proteger nuestras cuentas bancarias es una responsabilidad que comienza con algo tan sencillo como elegir una buena contraseña.



bancodonde.com