

De que se trata la doble autenticación, o ¿porque pedir algo más que un usuario y contraseña?

Doble autenticación, o autenticación de 2 factores (2FA) son **términos muy técnicos**. Lo que se esconde detrás de esto es básicamente **pedir algo más que un usuario y una contraseña**.

A diferencia de los VPNs y los programas de encriptación, este tipo de aplicaciones siempre **son gratuitas para incentivar su utilización**. De esta manera, todo el mundo gana: los comercios reciben menos quejas y reclamos, y las personas son menos vulneradas/hackeadas.

Nota: Al momento de implementar esta barrera de seguridad, se generará un **código de emergencia**. Es muy importante **siempre guardarlo emergencia que se genera, para el caso de que se pierda el celular o la PC en donde se genera este mecanismo**. De lo contrario, se perderá acceso definitivamente a las cuentas protegidas.

Cuatro maneras rápidas de implementar la doble autenticación (2FA)

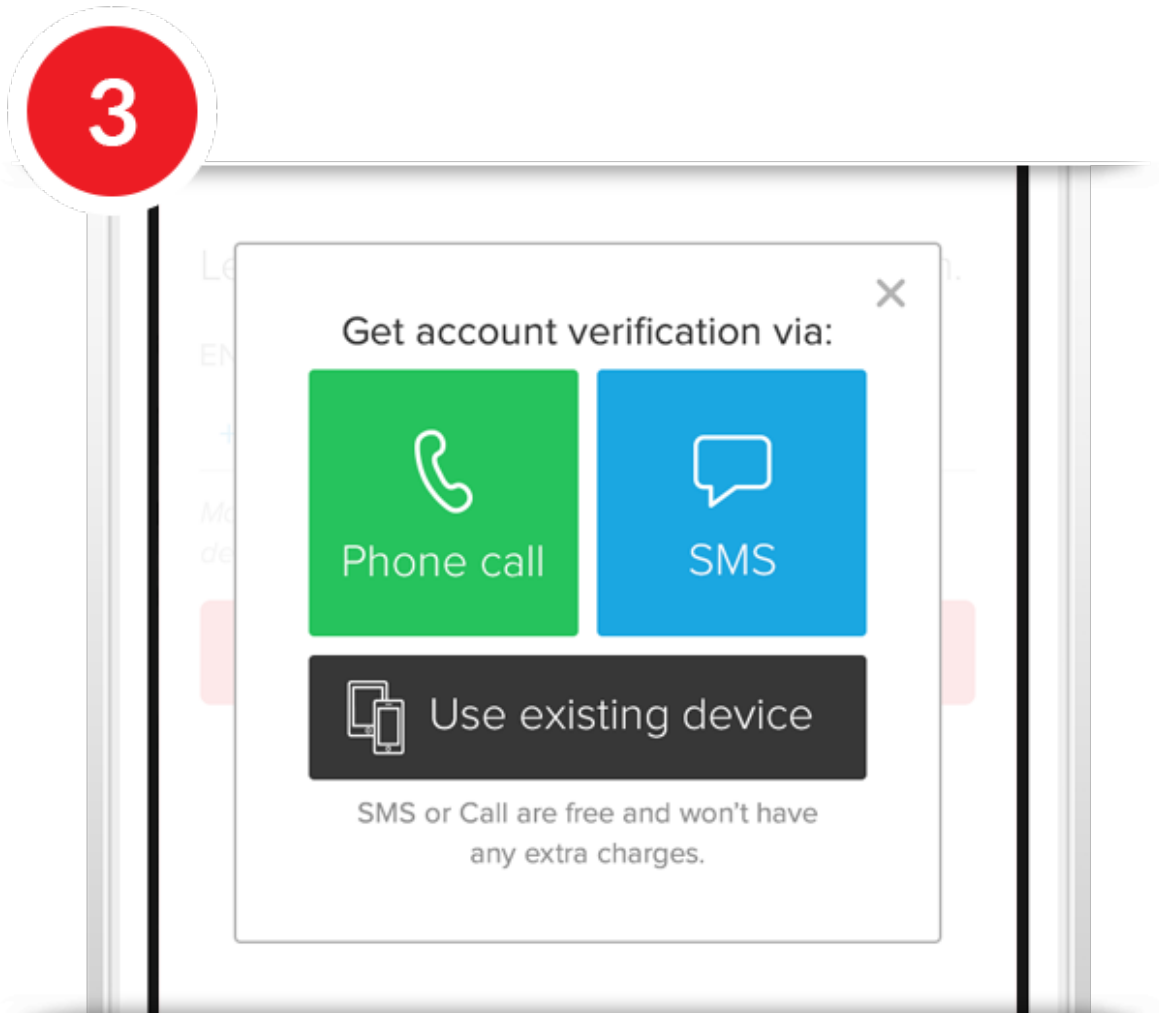
Te presentamos las cuatro opciones más comunes para activar este mecanismo, vamos de la menos segura a la más segura:

4. Código SMS

Con esta opción, cuando intentas entrar a una cuenta, simplemente se te envía a tu celular un código por SMS, generalmente de 4 a 6 dígitos. No es muy segura, porque podrían clonar tu celular, o interceptar ese código mediante antenas de telefonía ilegales.

3. Aplicación que se instala en tu PC o notebook

Con esta opción, instalas un programa que generará un código. [El software más común en esta categoría es Authy](#). Este software fue creado en el 2011 por [Daniel Palacio](#), y comprado por Twilio en febrero del 2014.



Así se ve la interfaz de Authy, cuando lo estás configurando

Esta opción no es la más segura, ya que en el caso de que te roben el dispositivo, podrían generar el código fácilmente.

2. Aplicación que se instala en tu celular

Esta opción es más segura, si el celular tiene clave de bloqueo y además hay un código que protege esta aplicación. Básicamente hay dos opciones muy populares que existen dentro de esta categoría, además de Authy:

Por un lado, esta Duo Mobile. Desarrollado por Duo Security Inc, una empresa actualmente adquirida por Cisco.



Duo Mobile

Duo Security, Inc. Negocios

Todos

Esta app es compatible con tu dispositivo.

Este es el link para descargarlo desde [Google Play \(para celulares con Android\)](#), y este es el [link para descargarlo desde la App Store de Apple](#).

Por otro lado, esta la app más masiva de Google.



Autenticador de Google

Google LLC Herramientas

Todos

Esta app es compatible con tu dispositivo.

Este es el link para descargarlo desde [Google Play \(para celulares con Android\)](#), y este es el [link para descargarlo desde la App Store de Apple](#).

1. Tokens físicos

Definitivamente, la opción más segura es tener una llave física ("token") que se transporta. Hay muchas variantes en cuanto a los mecanismos de funcionamiento.

Por ejemplo, en el caso de los tokens de Yubico, hay versiones que se conectan inalámbricamente para validar el ingreso a una cuenta, y otras versiones se conectan vía algún puerto USB,

para dar un código específico que solo esta dentro.