Autenticación de
dos factores y de dos pasos

Cuando se habla de autenticación de dos factores y autenticación de dos pasos, hablamos de capas adicionales que requieren un segundo paso o factor, además de la contraseña, para completar el acceso a una cuenta.
Esto disminuye el riesgo de accesos no autorizados a tus cuentas.
Además, actualmente la mayoría de plataformas y servicios digitales como Google, Facebook. Twitter, Amazon ya ofrecen estas opciones. Depende de ti activarlas.

¿Por qué es **buena idea usarlas?**

- Es **posible romper contraseñas cortas o predecibles.** Por lo que tener está opción hace más difícil el acceso a tus cuentas.
- Si utilizas **una contraseña para más de un acceso,** esto podría asegurar que si vulneran una de tus cuentas que tengan la misma contraseña, impida que vulneren otros accesos.
- Cuando hay **filtraciones de contraseñas** a gran escala.
- Si por error **accediste a un sitio falso** e introdujiste tu contraseña.
- Cada servicio **tiene sus propias vulnerabilidades,** activar esta opción puede ayudar a disminuir la probabilidad de que te afecten.

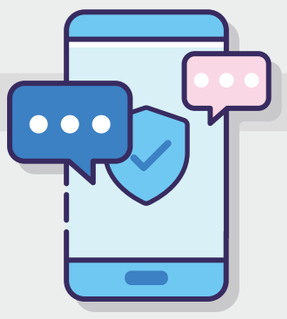
¿Cuál es la diferencia?

Autenticación **de 2 pasos**

Algo que sabes

Contraseña

Autenticación **de 2 factores**



Algo que sabrás

Un segundo código enviado por SMS, llamada telefónica, correo, etc.

Algo que tienes o que eres

Un móvil o una tableta previamente autorizados, desde los cuales autorizas o no, el acceso. O lecturas biométricas: huella dactilar, facial o de retina, por ejemplo.

Autenticación de dos factores y de dos pasos

¿Cómo **funcionan?** Regularmente:

Introduces una contraseña: Cada vez que accedas al servicio/cuenta ingresarás tu contraseña. Esta primera información será validada y de ser correcta, se enviará un segundo factor o un segundo paso de autenticación.

Información adicional: Luego del factor 1, te será solicitada información adicional de acuerdo a las opciones disponibles por el servicio:

— **Algo que sabes:** un código enviado al teléfono por medio de un mensaje de texto,

— **Algo que tienes:** una llave de seguridad física tipo usb, o

— **Algo que eres:** información biométrica proporcionada a algún sensor de tu dispositivo.

¿Cómo **lo configuro?**

Dependiendo de la aplicación o servicio, lo encontrarás en:
Configuración ⟶ Cuenta ⟶ Seguridad ⟶ Método de autenticación.

Beneficios

— Gestionas tu tranquilidad.

— Es gratuito y fácil.

— Protege la identidad.

— Detiene en gran medida los accesos no deseados.

— Disponible en muchos servicios actualmente.

¿Me quitará **mucho tiempo?**

Es verdad que añade tiempo extra cuando intentas acceder a tus cuentas, a la vez puede **ahorrarte tiempo y ratos de angustia por intentos de acceso no autorizado a tus dispositivos o cuentas.** Depende de la paciencia, disposición y voluntad de ocupar unos segundos extra para asegurar un mayor nivel de seguridad y sobre todo de tranquilidad.

ARTICLE 19

Fuentes:
https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/,
https://www.google.com/intl/es-419/landing/2step/,
https://es.wikipedia.org/wiki/Autenticaci%C3%B3n_de_m%C3%BAltiples_factores#Factores_de_conocimiento,
https://twofactorauth.org/ — conocer qué servicios ofrecen 2fa. https://www.telesign.com/turnon2fa/tutorials/ - tutoriales de 2fa