NJSBA
PRACTICEHQ
PREPARED BY
Affinity
CONSULTING

TWO FACTOR AUTHENTICATION

This is also known as 2FA or multi factor authentication

WHAT IS TWO FACTOR AUTHENTICATION?

Here's a good definition.

> "Two-factor authentication (2FA), sometimes referred to as *two-step verification* or *dual-factor authentication*, is a security process in which users provide two different authentication factors to verify themselves."[1]

Two-factor authentication provides an additional layer of security and makes it harder for attackers to gain access to a person's devices and online accounts, because knowing the victim's password alone is not enough to pass the authentication check. Two-factor authentication has long been used to control access to sensitive systems and data, and online services are increasingly introducing 2FA to prevent their users' data from being accessed by hackers who have stolen a password database or used phishing campaigns to obtain users' passwords.

The ways in which someone can be authenticated usually fall into three categories known as the factors of authentication, which include:

KNOWLEDGE FACTORS

A knowledge factor is something the user knows, such as a password, PIN or shared secret.

POSSESSION FACTORS

Possession factors are something the user has, such as an ID card, security token or a smartphone.

INHERENCE FACTORS (AKA BIOMETRICS)

Biometrics are something the user is, something inherently about him or her. "These may be personal attributes mapped from physical characteristics, such as fingerprints, face and voice. It also includes behavioral biometrics, such as keystroke dynamics, gait or speech patterns."[2]

DISCOVER WHICH SERVICES USE TWO FACTOR AUTHENTICATION

Visit the 2FA Directory to get an idea of which services you use offer two factor authentication.

A PLACE TO STORE YOUR SECOND FACTORS

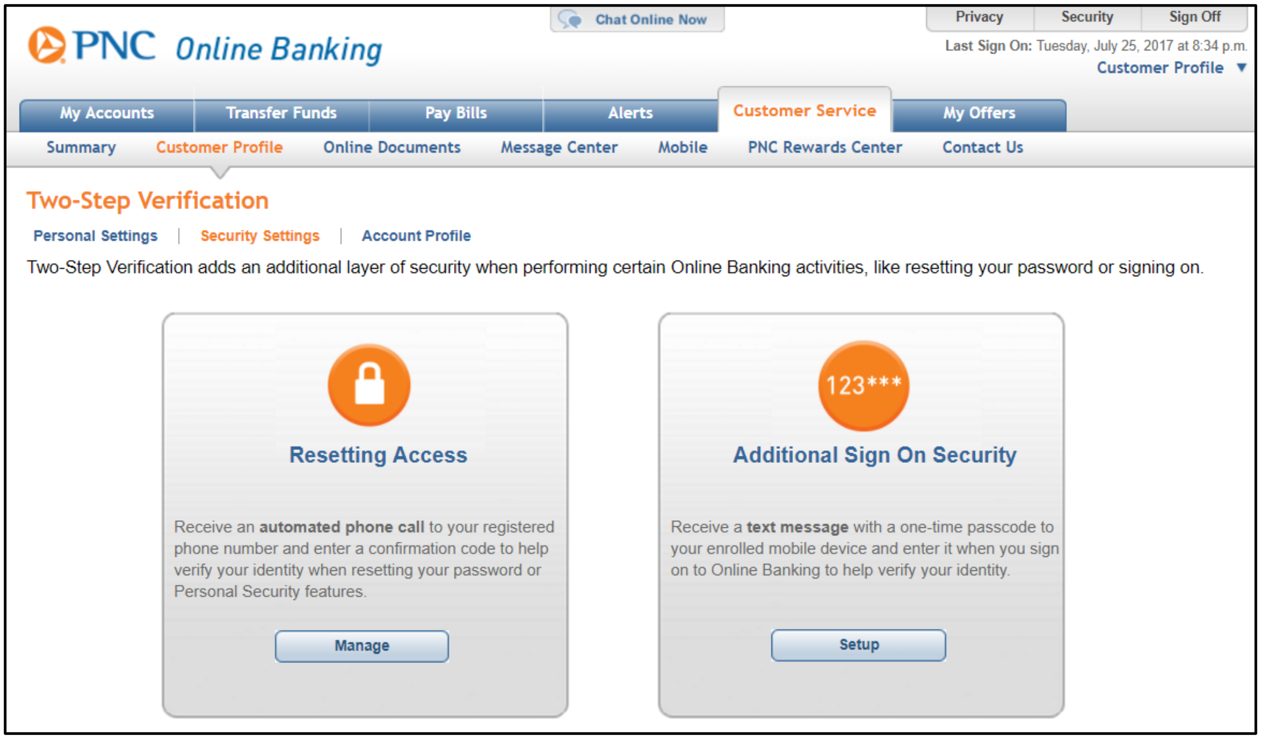
1Password, Dashlane, and Roboform support storing 2FA codes in their password managers. If you're using another program, you'll need an app like Google Authenticator, Microsoft Authenticator, or Twilio's Authy.

[1] Linda Rosencrance, "Two-Factor Authentication," TechTarget, accessed March 31, 2023, http://searchsecurity.techtarget.com/definition/two-factor-authentication.

[2] Ibid.

HOW DO YOU GET 2FA?

For critical services you access online, check to see if they offer any type of 2FA. Keep in mind that 2FA is ANNOYING, but better security is almost always more annoying. If you want to protect yourself well, be prepared to be slightly annoyed. Anyway, here are some 2FA ideas. Your bank probably offers it:



Last Sign On: Tuesday, July 25, 2017 at 8:34 p.m.

Two-Step Verification

Two-Step Verification adds an additional layer of security when performing certain Online Banking activities, like resetting your password or signing on.

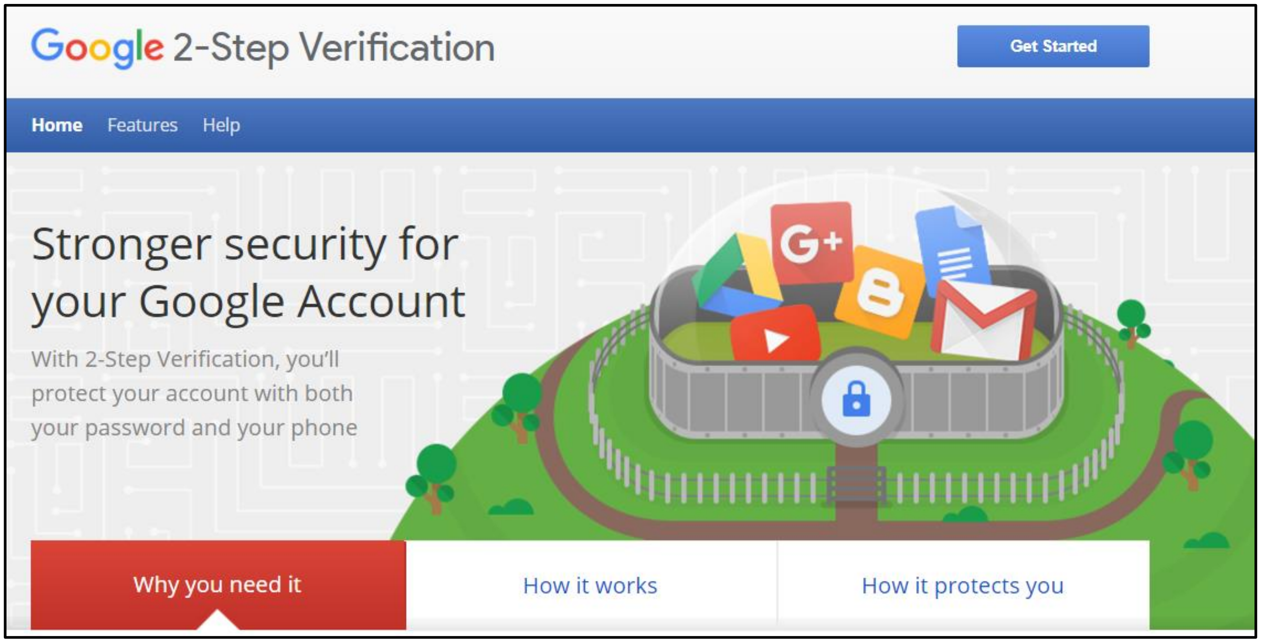
Resetting Access

Receive an **automated phone call** to your registered phone number and enter a confirmation code to help verify your identity when resetting your password or Personal Security features.

Additional Sign On Security

Receive a **text message** with a one-time passcode to your enrolled mobile device and enter it when you sign on to Online Banking to help verify your identity.

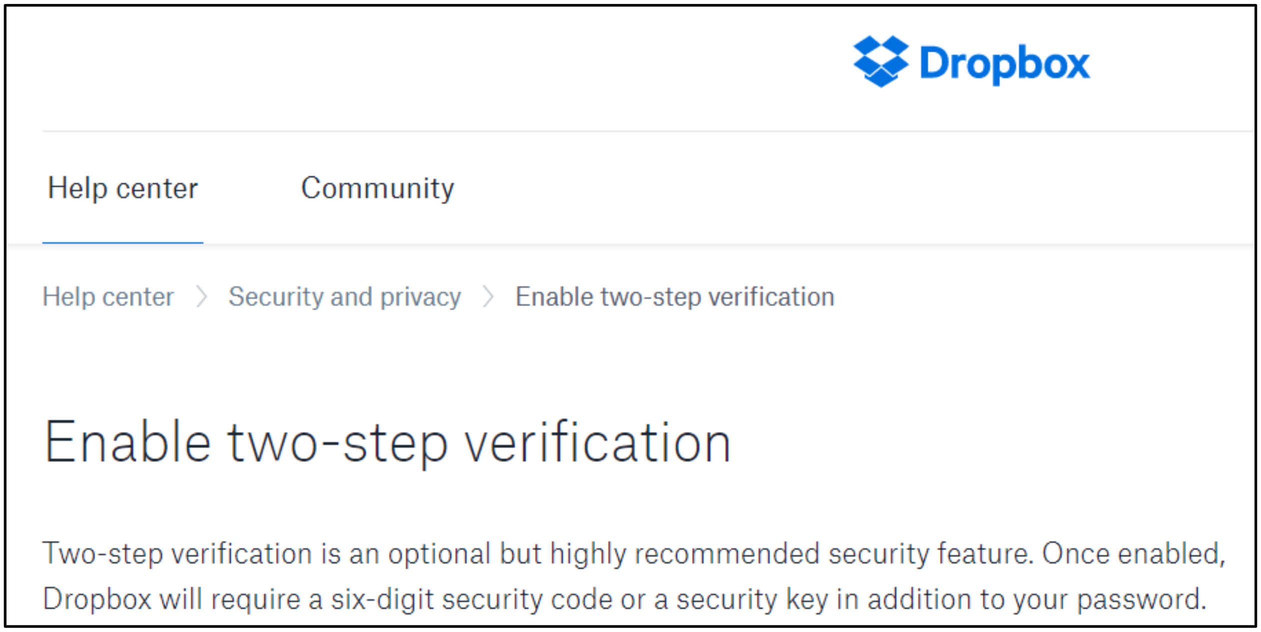
Your email account probably offers it:



Stronger security for your Google Account

With 2-Step Verification, you'll protect your account with both your password and your phone

Your file sharing service probably offers it:



Dropbox

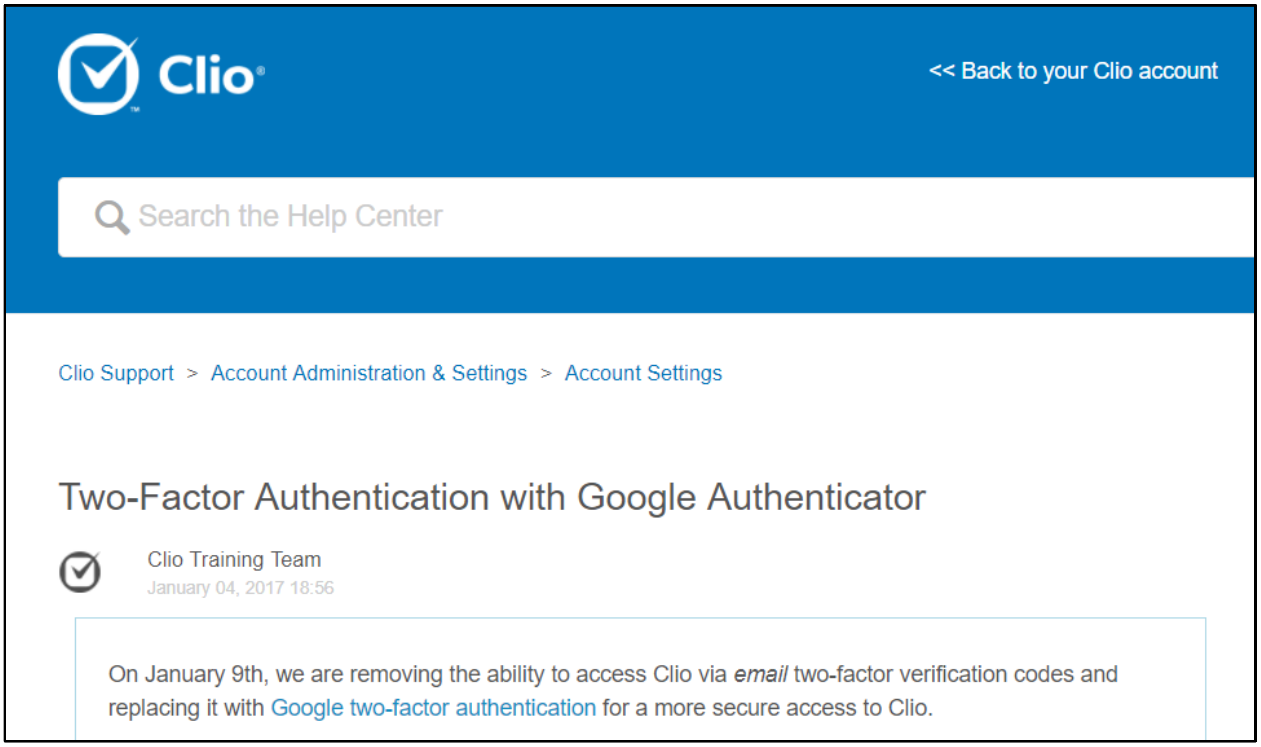
Help center   Community

Help center > Security and privacy > Enable two-step verification

Enable two-step verification

Two-step verification is an optional but highly recommended security feature. Once enabled, Dropbox will require a six-digit security code or a security key in addition to your password.

Your case management system probably offers it:



Clio

<< Back to your Clio account

Search the Help Center

Clio Support > Account Administration & Settings > Account Settings

Two-Factor Authentication with Google Authenticator

Clio Training Team
January 04, 2017 18:56

On January 9th, we are removing the ability to access Clio via *email* two-factor verification codes and replacing it with Google two-factor authentication for a more secure access to Clio.