Two Factor Authentication

This is also known as 2FA or multi factor authentication.

1. **What Is Two Factor Authentication?** Here's a good definition.

   "Two-factor authentication (2FA), often referred to as two-step verification, is a security process in which the user provides two authentication factors to verify they are who they say they are. 2FA can be contrasted with single-factor authentication (SFA), a security process in which the user provides only one factor -- typically a password.

   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:

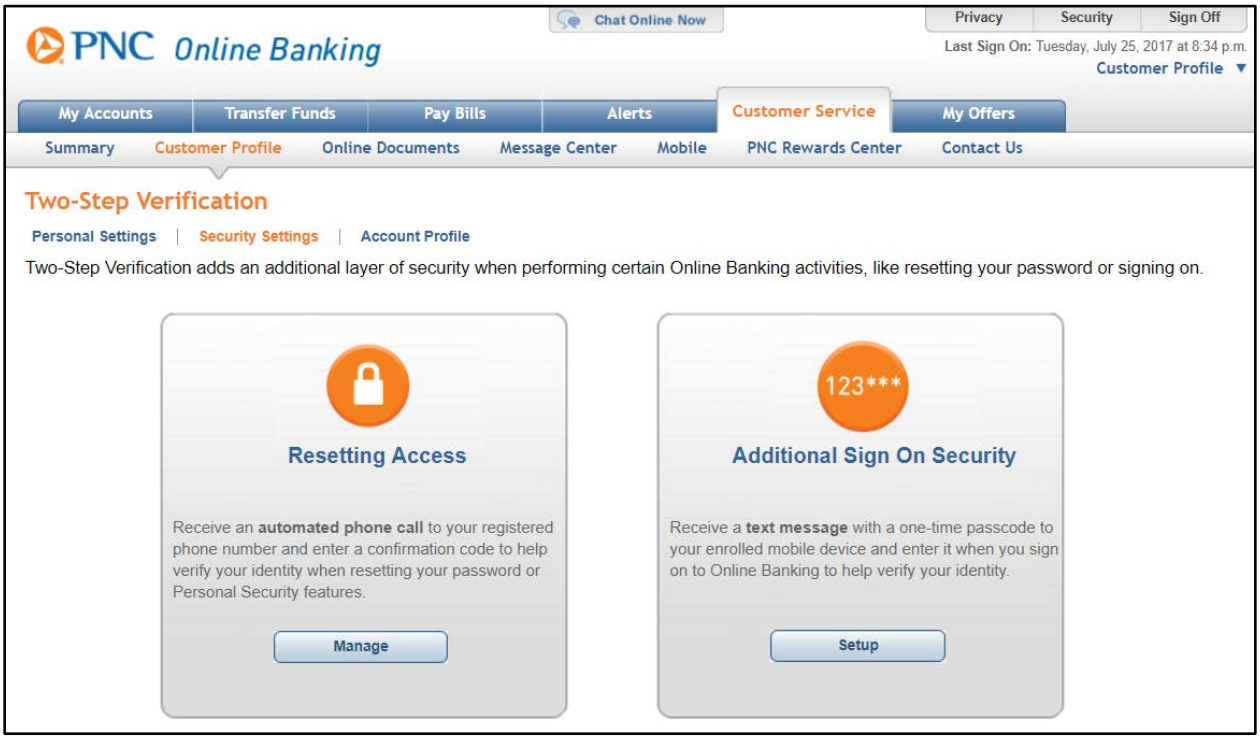
   1. **Knowledge factors** -- something the user knows, such as a password, PIN or shared secret.

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

   3. **Inherence factors, more commonly called biometrics** -- something the user is. These may be personal attributes mapped from physical characteristics, such as fingerprints, face and voice. It also includes

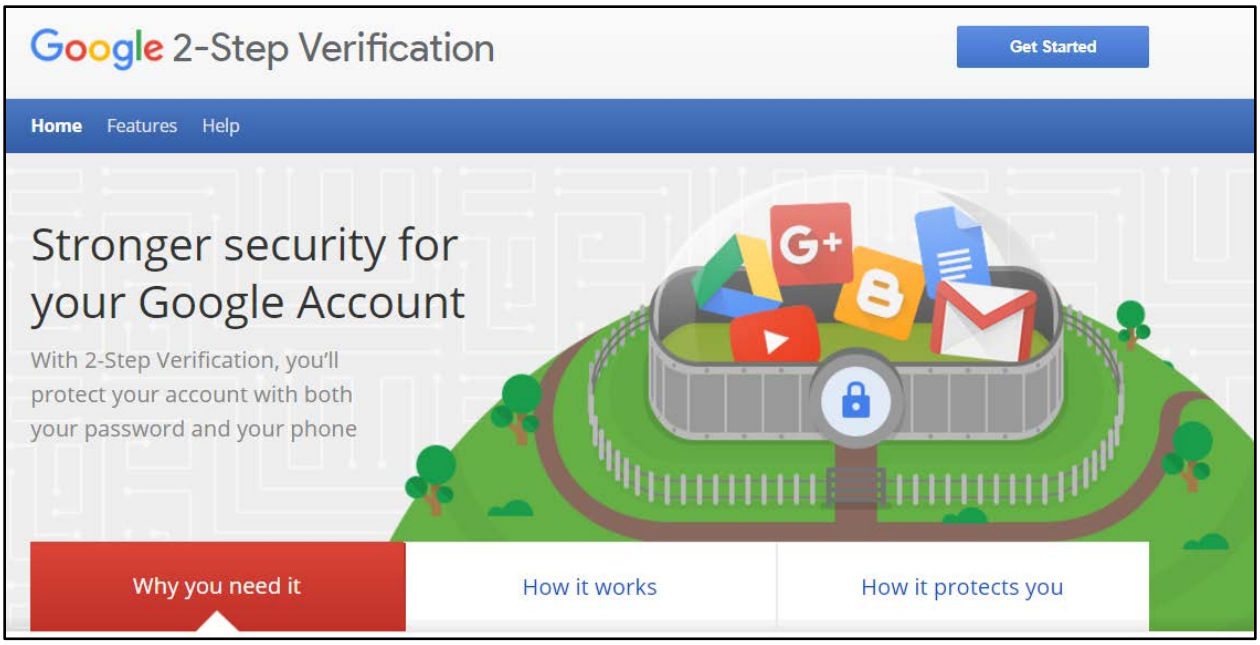
behavioral biometrics, such as keystroke dynamics, gait or speech patterns."[1]

2. **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:

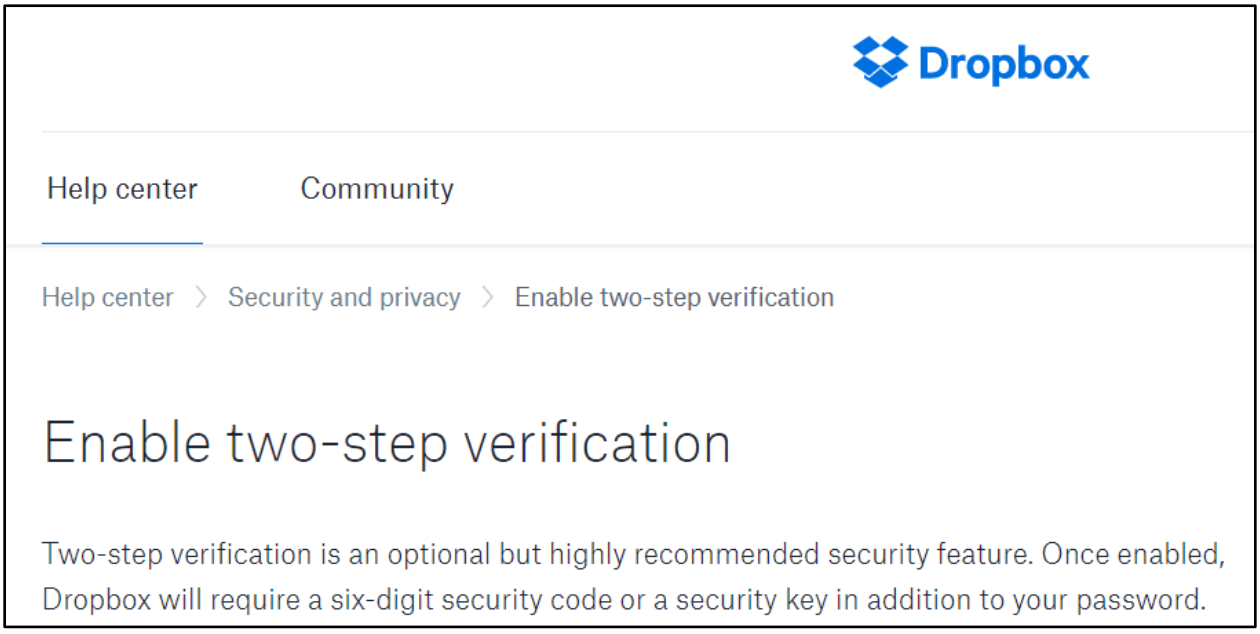


Your email account probably offers it:

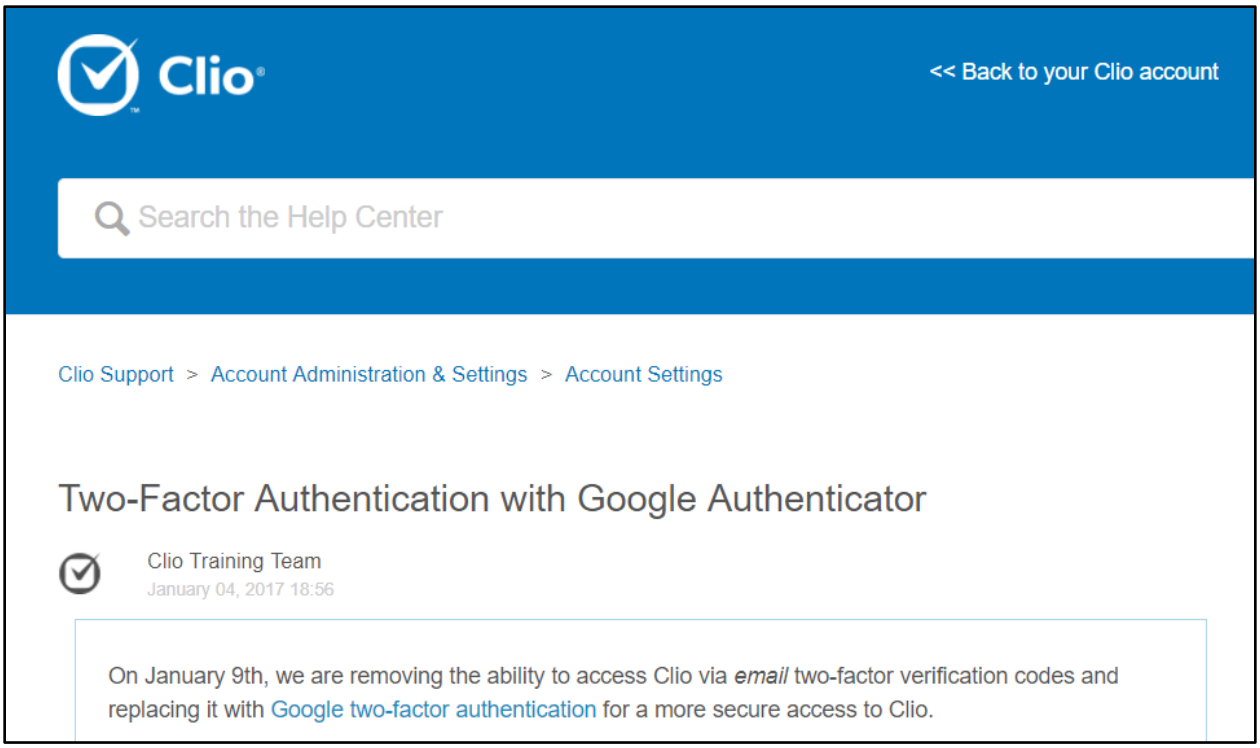
[1] See http://searchsecurity.techtarget.com/definition/two-factor-authentication



Your file sharing service probably offers it:



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.