

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), 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:

KNOWLEDGE FACTORS -- SOMETHING THE USER KNOWS, SUCH AS A PASSWORD, PIN OR SHARED SECRET.

POSSESSION FACTORS -- SOMETHING THE USER HAS, SUCH AS AN ID CARD, SECURITY TOKEN OR A SMARTPHONE.

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

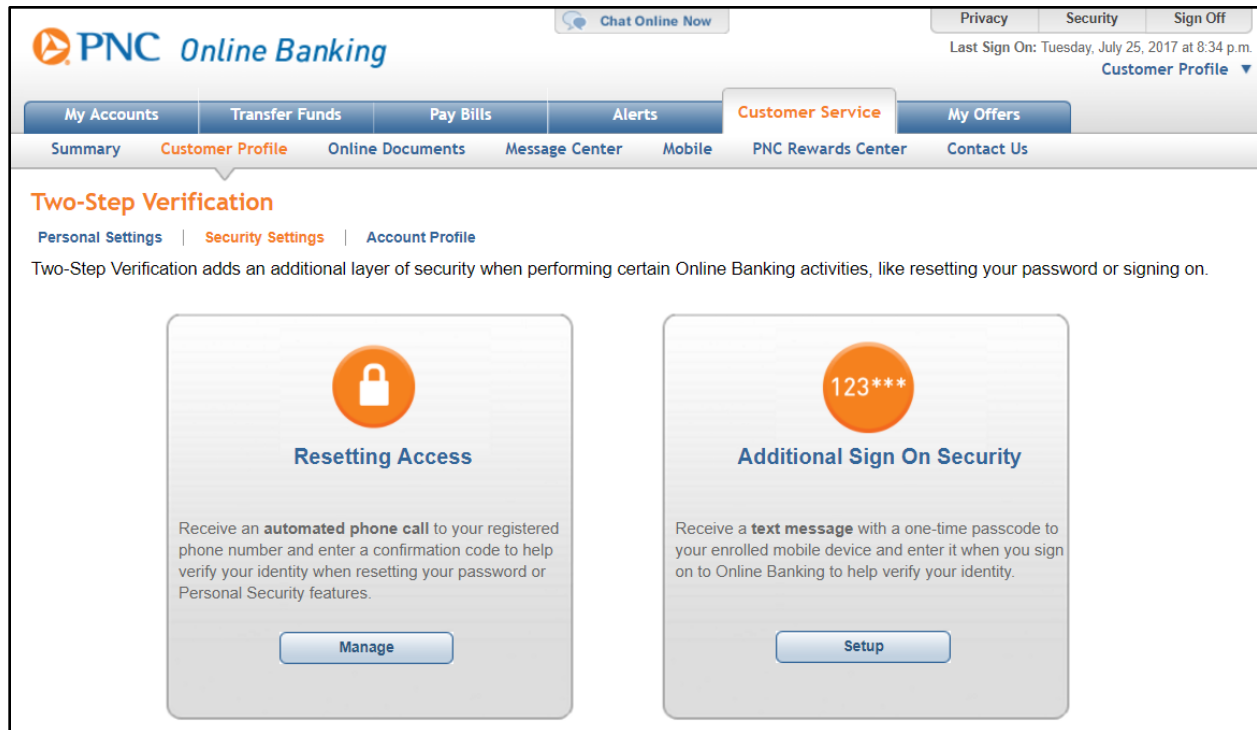
DISCOVER WHICH SERVICES USE TWO FACTOR AUTHENTICATION

Visit <https://twofactorauth.org> to get an idea of which services you use offer two factor authentication.

¹ See <http://searchsecurity.techtarget.com/definition/two-factor-authentication>.

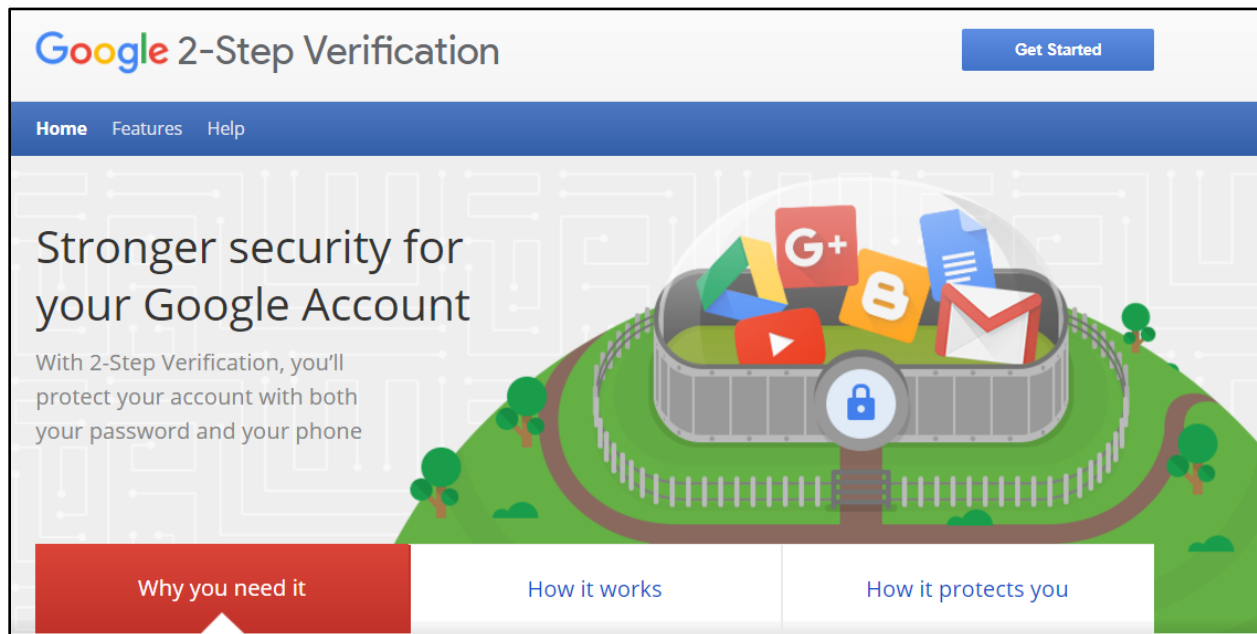
HOW DO YOU GET 2FA?

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:



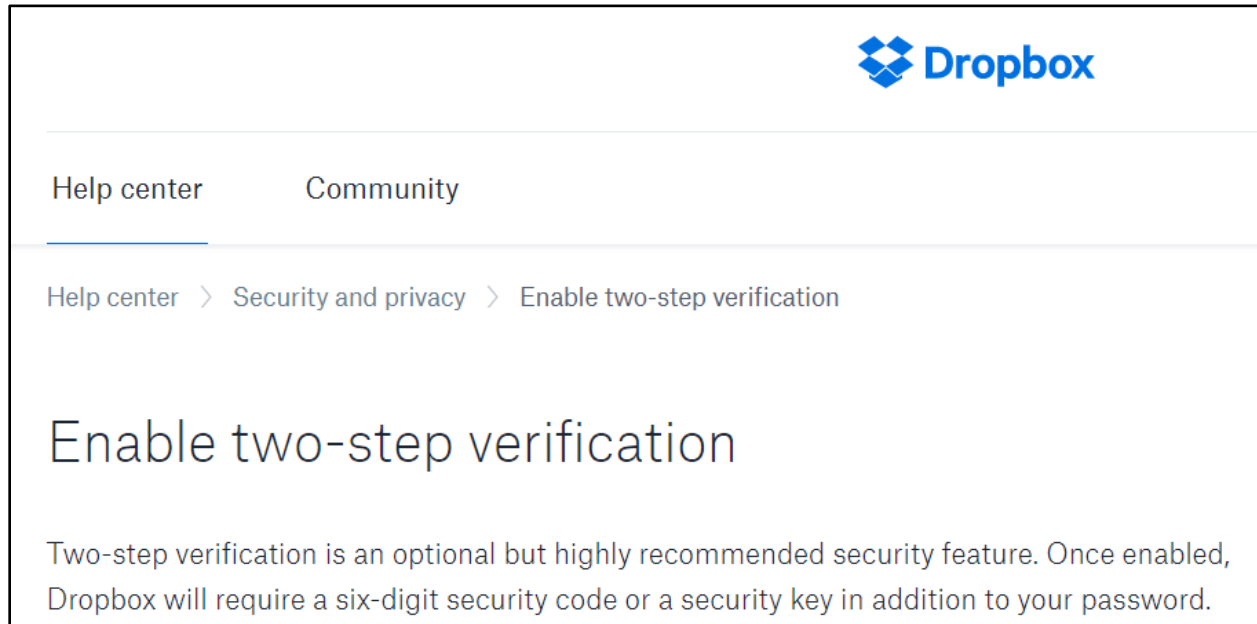
The screenshot shows the PNC Online Banking interface. At the top, there's a navigation bar with links for "My Accounts", "Transfer Funds", "Pay Bills", "Alerts", "Customer Service", and "My Offers". Below this is a secondary navigation bar with "Summary", "Customer Profile", "Online Documents", "Message Center", "Mobile", "PNC Rewards Center", and "Contact Us". The main content area is titled "Two-Step Verification" and includes links for "Personal Settings", "Security Settings", and "Account Profile". A sub-header states: "Two-Step Verification adds an additional layer of security when performing certain Online Banking activities, like resetting your password or signing on." There are two main cards: "Resetting Access" with a padlock icon and a "Manage" button, and "Additional Sign On Security" with a "123***" icon and a "Setup" button. The "Resetting Access" card text says: "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." The "Additional Sign On Security" card text says: "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:



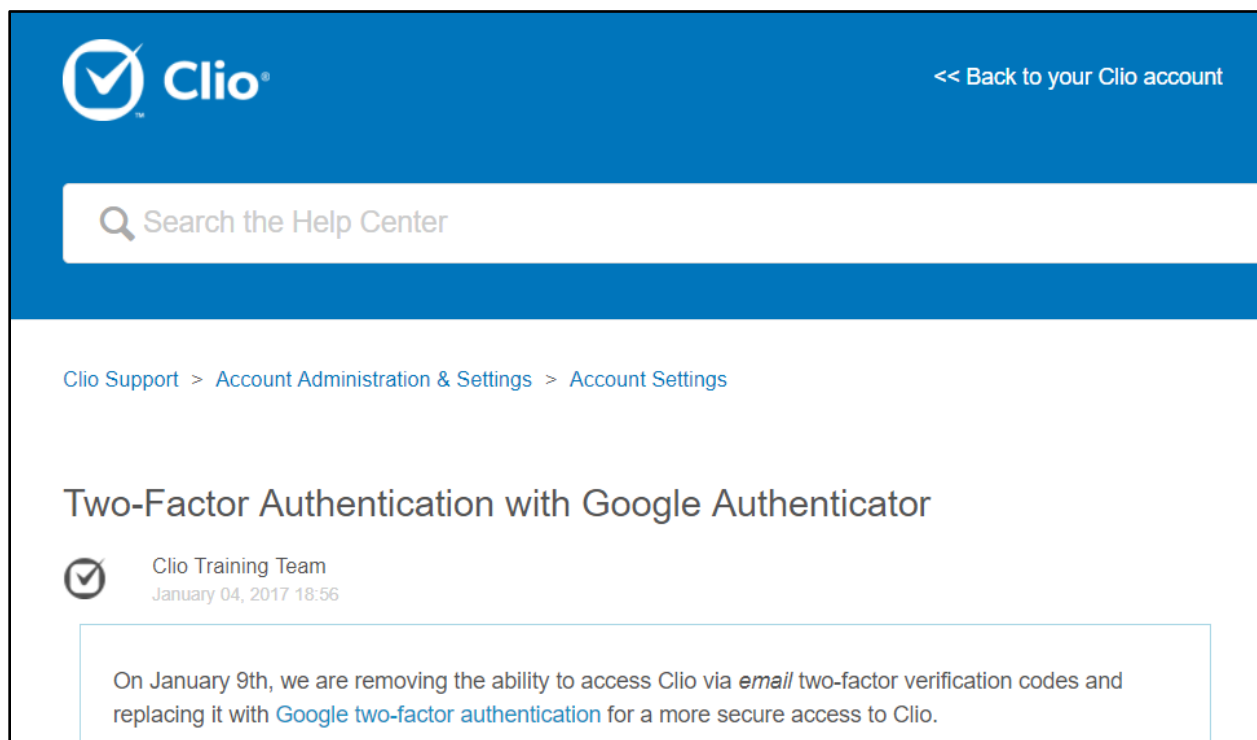
The screenshot shows the Google 2-Step Verification landing page. At the top, it says "Google 2-Step Verification" with a "Get Started" button. Below is a navigation bar with "Home", "Features", and "Help". The main heading is "Stronger security for your Google Account". Below this, it says: "With 2-Step Verification, you'll protect your account with both your password and your phone". To the right is an illustration of a castle with a lock icon, surrounded by Google icons (G+, B, YouTube, Mail). At the bottom, there are three tabs: "Why you need it" (highlighted in red), "How it works", and "How it protects you".

Your file sharing service probably offers it:



The screenshot shows the Dropbox Help Center interface. At the top right is the Dropbox logo. Below it are navigation links for 'Help center' and 'Community'. A breadcrumb trail reads 'Help center > Security and privacy > Enable two-step verification'. The main heading is 'Enable two-step verification'. Below the heading, a paragraph states: '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:



The screenshot shows the Clio Help Center interface. At the top left is the Clio logo, and at the top right is a link '<< Back to your Clio account'. Below the header is a search bar with the placeholder text 'Search the Help Center'. A breadcrumb trail reads 'Clio Support > Account Administration & Settings > Account Settings'. The main heading is 'Two-Factor Authentication with Google Authenticator'. Below the heading, there is a post from the 'Clio Training Team' dated 'January 04, 2017 18:56'. The post content is enclosed in a light blue box and reads: '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.'