2-Factor RSA

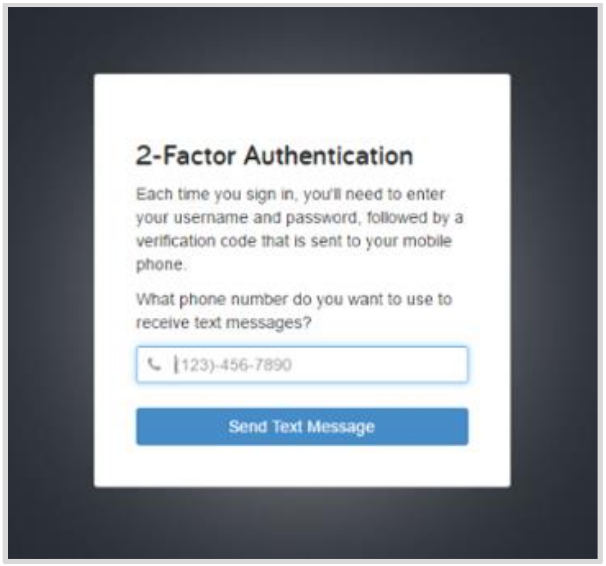
This guide will outline the 2-Factor Authentication integrated in your Personal Financial Management Website! The main purpose of 2FA is to protect the security of your information. 2FA will verify your identity using a PIN sent to your phone. This is an important measure in safeguarding your personal financial data, a matter we take very seriously. There are two levels of security to choose from – **Standard** or **High**.

Standard Security: you are only required to enter a PIN when "at –risk activity" has been identified. Choose this option if you prefer to only be prompted with additional security when our system detects a potential threat (e.g. a log in from a foreign country).

High Security: you are required to enter a PIN every time you log in. Choose this option if you prefer to use the highest level of security available.

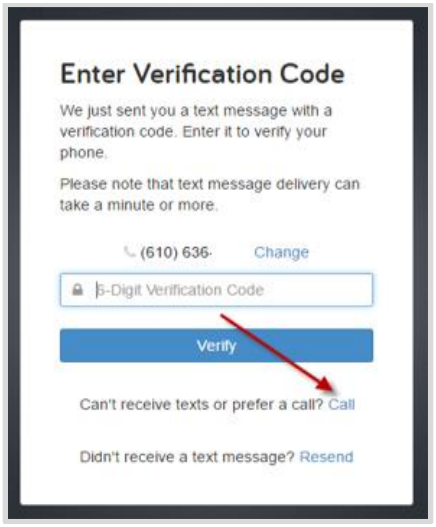
Initial Enrollment

1. Upon logging in, you will be required to register a primary phone number to be used for 2FA verification. Enter your phone number and click **Send Text Message**. If you enter a landline, you will receive a phone call that reads your PIN to you. For international phones, add a "+" in front of your number.

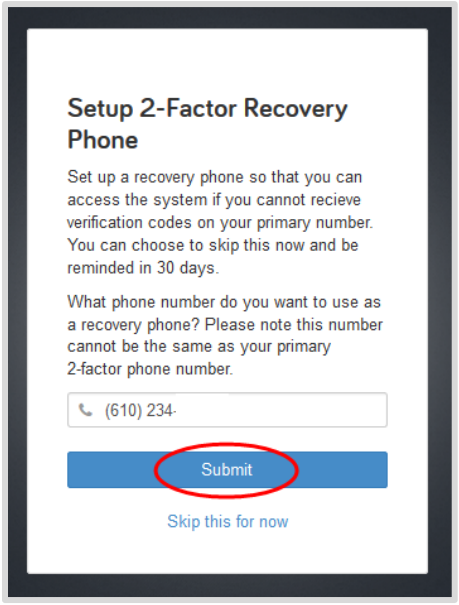


2-Factor RSA

2. Once you have received your PIN, enter the 6 digit code into verification box and click **Verify**. Click the Call link to have the verification code read to you over a phone call. The code expires after 10 minutes, click the Resend link to receive a new PIN verification code.



3. Next you will be prompted to set up a recovery phone. This number will be used if you do not have access to your primary phone while trying to login.

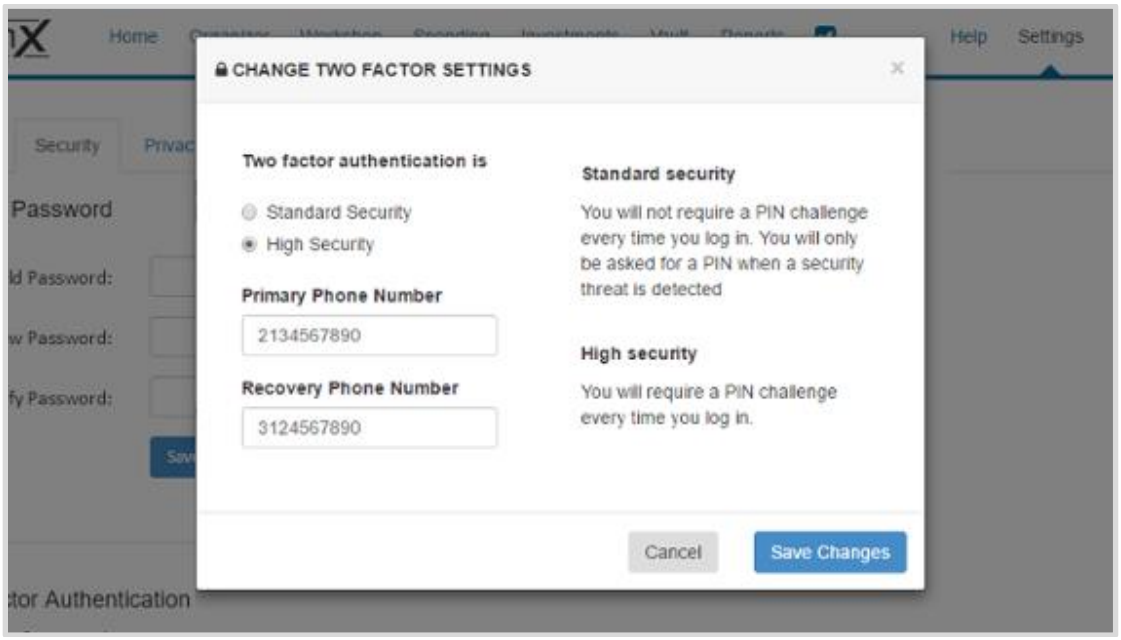


Note: Do not use the same number as your Primary Phone.

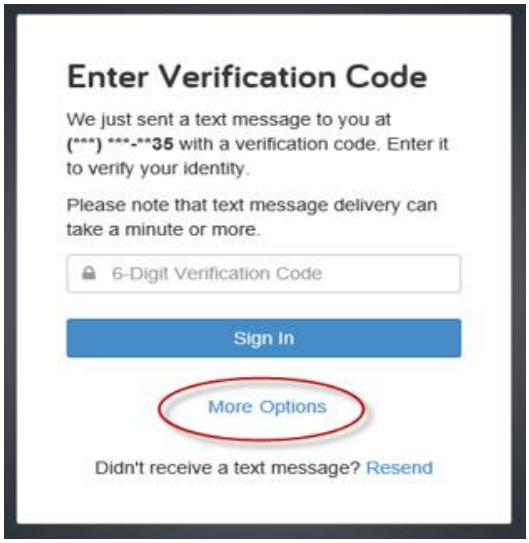
2-Factor RSA

Settings & Subsequent Logon

4. Your settings will dictate whether or not you are required to enter a PIN on every login (High Security) or only when a potential threat is detected (Standard Security.) To change your security settings, click the **Settings** link in the top right of your website. From there, choose **Security** to manage your 2-Factor settings.



5. If you opt for High Security, you will generate a *new* PIN for every logon. The logon screen will prompt you to enter the 6 digit code. Click **More Options** to receive a code on your recovery phone.

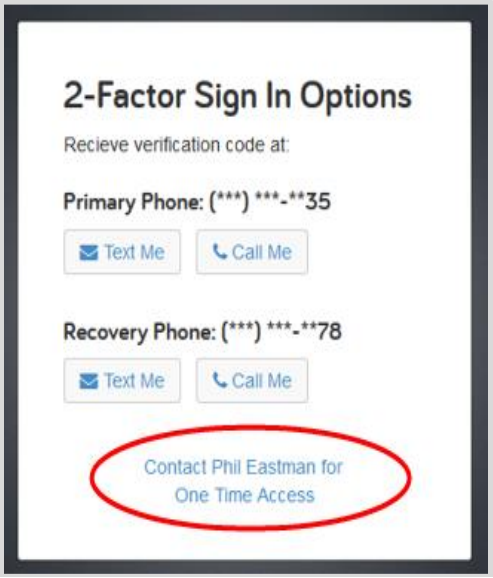


2-Factor RSA

Troubleshooting

- You will have 3 attempts to correctly verify your PIN. If entered incorrectly 3 times, your account will then be **locked**. In order to unlock your account, please call the manager of your Personal Financial Website.

- If you do not have access to either your Primary or Recovery phones, you are able to gain access to your website by using a **One Time Verification Code**. From your 2-Factor Sign In Options, click the link to Contact your Representative for One Time Access.



Next, call your Financial Representative and provide them with the code provided on your screen. The One Time Access code will change after each use.