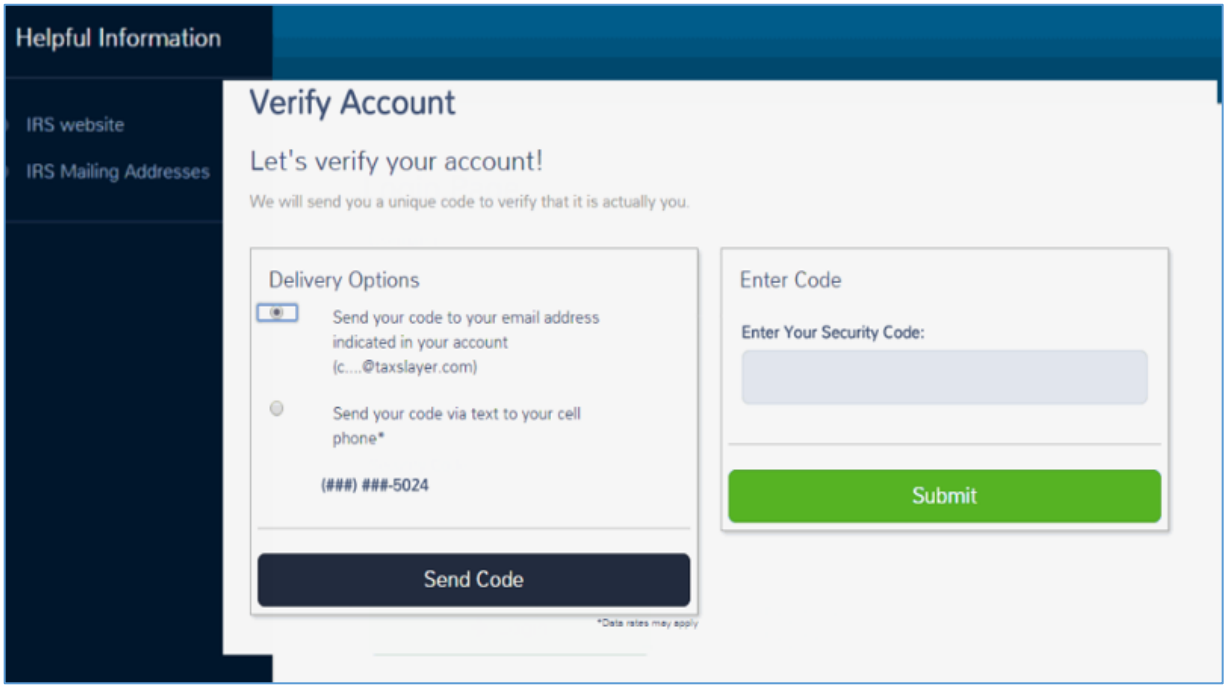
# Multi-Factor Authentication (MFA) for TSO

*AARP Foundation National Technology Committee*

**Summary:** Multi-Factor Authentication (MFA) is an increasingly used security measure that will be implemented for TaxSlayer Online (TSO) user logins. The MFA challenge will be the last step when a user signs in to TSO under certain conditions. The necessary code is provided to the user via a text message or an email message.

**When MFA Will Be Required:** TaxSlayer will begin using the MFA procedure when tax returns can be created. MFA challenges will be presented to a TSO user the first time that user logs onto the system using a new computer and periodically thereafter as set by the site's Admin user (7 to 90 days). ***The setting of the period for MFA challenges is not available as of 1/15/2017.*** When it is, information on how to set or change the challenge frequency will be included in the NTC Setup Guide for TaxSlayer Pro Online on OneSupport (NTC Setup Guide).

**How MFA Works:** When MFA is required, the challenge screen will be displayed:




The user should select the method of delivery for the Security Code - either the email or cell phone number that has been entered in TSO for that user. Click Send Code, and the code should be received shortly. **Codes will expire after a certain period (likely 15 minutes), so it is important that the user enter the code promptly after receipt**.

User email and cell phone information is entered by the site Admin during preparer setup (user creation). Neither the email address nor the cell phone number are required to be unique for each user, but it is recommended that they be unique. Both the email and cell phone information can be changed later by the Admin, but not by any other user. See the NTC Setup Guide for more information about preparer setup.

# Multi-Factor Authentication (MFA) for TSO

*AARP Foundation National Technology Committee*

**Potential Issues Related to MFA:**

1) **Use of the same cell phone number for more than one user at a site:** MFA security codes do not identify the user that they are associated with. If the same cell phone number is used for multiple site users, it will not be clear which user a security code belongs to unless the users login in a clearly identified order. Additionally, those users will not be able to use MFA by text message when they are away from the owner of the cell phone.
2) **Poor cell phone reception at site:** This could affect the ability of users to receive codes by text message. Be sure the cell phone works at the site before your first tax prep day.
3) **Use of the same email address for more than one user at a site.** Email is used for both MFA Security and password recovery. We believe that, as with text messages, the user name will not be identified in the email code message from TaxSlayer. In addition, users will not be able to use either of these functions if the email account owner is not present.
4) **Problems accessing email:** Some volunteers may have difficulty accessing their personal email account to retrieve the code. This might occur if they cannot remember their webmail site and/or password or if they have implemented security measures that require authentication whenever a new device is used to sign into the email account.
    a. All users should test whether they can access their email using their tax preparation computer BEFORE going to the site for the first time or at least the first time they go to the site. This should allow them to work through any device authentication issues ahead of time. Users can also bookmark their email provider's site for convenient access later.
    b. Some users may not want to access their personal email accounts for the purpose of MFA or password reset. This is especially true if using site-provided computers. In this case, a potential solution is for the Admin user to establish web-based email accounts on Gmail, Yahoo, etc. for these volunteers that will only be used for TSO purposes and to use these accounts when setting up each TSO user. These users can then be furnished with the login information for their email account so they can retrieve security codes and perform password reset themselves.