One-e-App (OEA) Tips Sheet – Login Captcha and Two Step Verification
March 2019

The purpose of this Tips Sheet is to:

1. Explain the change to the OEA system that add enhanced security features which becomes effective <mark>April 4, 2019</mark>: Captcha and Two Step Verification (2SV).

2. Explain that this change to the OEA system requires that each OEA user have a valid agency email address in their OEA account profile.

   BACKGROUND: One-e-App vendor Social Interest Solutions (SIS) implemented two enhancements to the OEA login security environment - They are the Captcha challenge and the Two Step Verification (2SV).

1. **CAPTCHA CHALLENGE AT LOGIN:** The OEA log-in screen has added a Captcha challenge feature (a series of computer generated characters). Users must enter their login User ID, Password, Captcha Code and click on 'Sign-in'.


2. **TWO STEP VERIFICATION:** The next screen, the 2SV will be a conditional page, meaning it will only appear if the user's account meets one the following verification conditions*:

   • A user's first visit to the OEA site
   (After 2SV goes 'live', all users will be considered first time visitors of the OEA site and be be required to provide 2SV).
   • A user's password expires
   • A user changes their password
   • A user's account has been locked due to inactivity or too many invalid attempts at login
   • A user elects to not remember their device
   • A user's is attempting to log on from an unknown location

If and when a user's account meets one of the verification check conditions, the user will be sent a six-digit numeric pin code via email. The pin code will be sent to the email address provided at the time of the user's account creation.

IMPORTANT: Implementation of the 2SV security feature will require that all OEA users (including those logging in from a remote computer) have access to the email address listed on their OEA profile. If your email address changes, please ensure that you change it in your OEA user profile. Refer to Page 3 for instructions.
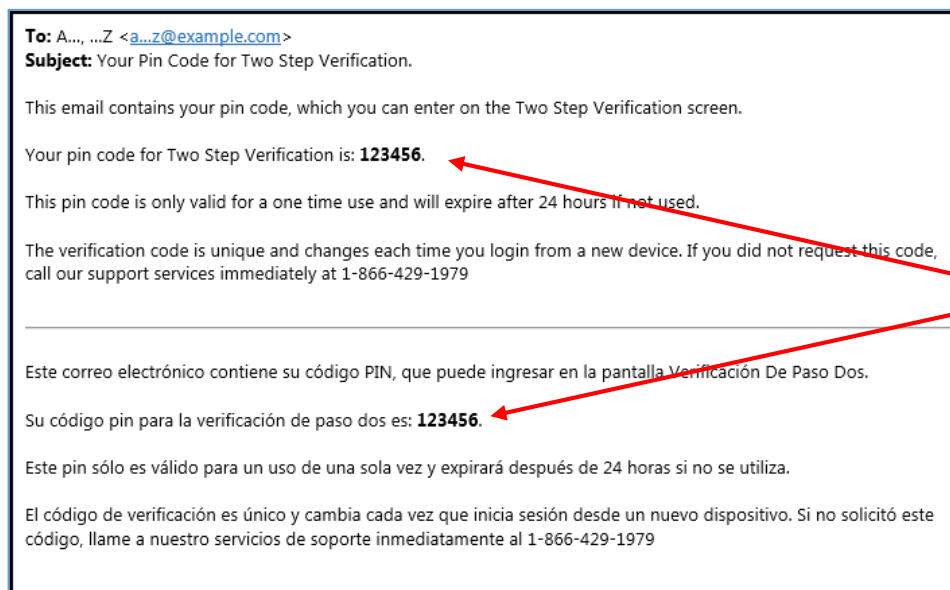
Example of the Six-digit numeric pin code message sent to user's email address in English and Spanish.

3. **VERIFY YOUR IDENTITY SCREEN:** Appears after Sign in' on the Login screen.

'Verify Your Identity' screen - Copy & paste or key in the pin code here.

Check 'Yes' to remember your computer. 2SV will only be required again if it meets one of the verification conditions*.

Once 2SV is completed for each up to three computers, 2SV will only be required again if it meets one of the verification conditions*.

Check 'No' will require 2SV upon each subsequent login attempt.

INSTRUCTIONS FOR CHANGING EMAIL ADDRESS ON OEA PROFILE: From your OEA Dashboard screen under 'My Account'.

Click on Modify My Profile link.

Your profile can be modified at this screen.
Change your email address.

4. **CLICK NEXT:** After you've changed your profile to include your new email address, click 'Next' **through all subsequent screens** until you land on your Dashboard. Your profile changes will be saved.

5. **INSTRUCTIONS TO COMMUNITY PARTNER INFORMATION SYSTEMS:** In preparation for the implementation of the 2 Step Verification (2SV) process in the One-e-App tool, Social Interest Solutions is requesting that each Community Partner using OEA reach out to their respective IT Department(s) and request that **'support@oneeapp.org'** be added to their email White List. This is the email address that OEA will use to send the verification pin codes to individual users for the 2SV process.

By adding this email address to the White List it will help to ensure that 2SV verification emails are not directed to the user's Spam or Junk mail folders.

If you have any questions about the contents of this Tips Sheet, please contact your Program Advocate.

<div align="center">

CAPTCHA AND TWO STEP VERIFICATION QUESTIONS & ANSWERS:

</div>

Q: When will a OEA user be required to complete the 2SV process?

A: 2SV is a conditional check and will only appear under one of the following conditions:

- *A user's password expires*
- *A user changes their password*
- *A user's account has been locked due to inactivity or too many wrong attempts at login*
- *A user elects to not remember their device*
- *A user is attempting to log on from an unknown location.*

Q: If a OEA user has previously completed 2SV on three separate computers and then the account becomes disabled or inactivated, will the user have to complete 2SV on all three computers once the account is reactivated?

A: Yes, the user will have to complete the 2SV process on all previously 'recognized' computers.

Q: Is it possible for OEA 2SV to 'recognize' more than three computers?

A: No. Following security best practices, OEA has set the limit to recognize a maximum of three computers. This reduces the chances that a bad actor can use a computer and retrieve the cookie to bypass the 2SV screen. Even if the number of computers was expanded and the computer was not used for extended period of time, that stored cookie will expire which will then result in the need for 2SV.

Q: Is it possible to have 2SV apply only to enrollers such as CECs and CEC Supervisors, and exclude Read-only users?

A. No. 2SV is a security feature which will need to be applied to all users types equally, especially because a single user account may have multiple user types associated with it.