# Authenticator Help

## Why 2-Factor Authentication?

The Canadian Occupational Performance Measure requires 2-factor authentication in order to further secure your clients personal information. This means that any person attempting to gain access to an account will require not only your username and password, but also a verification code that you will set up on your mobile device.

## How Does It Work?

The first time you login to the COPM Web-App, you will encounter a second login page (*fig.1*), titled *VERIFY*. This is where you will complete your 2-factor authentication by obtaining a 6-digit verification code from *Google Authenticator* - a free program you will set up on your mobile phone or tablet. Submitting the correct 6-digit code will complete the login process. The 6-digit code provided by *Google Authenticator* changes every 30 seconds, providing a great deal more security than a traditional username and password. Even if your login information is stolen, it will no longer function after half a minute.

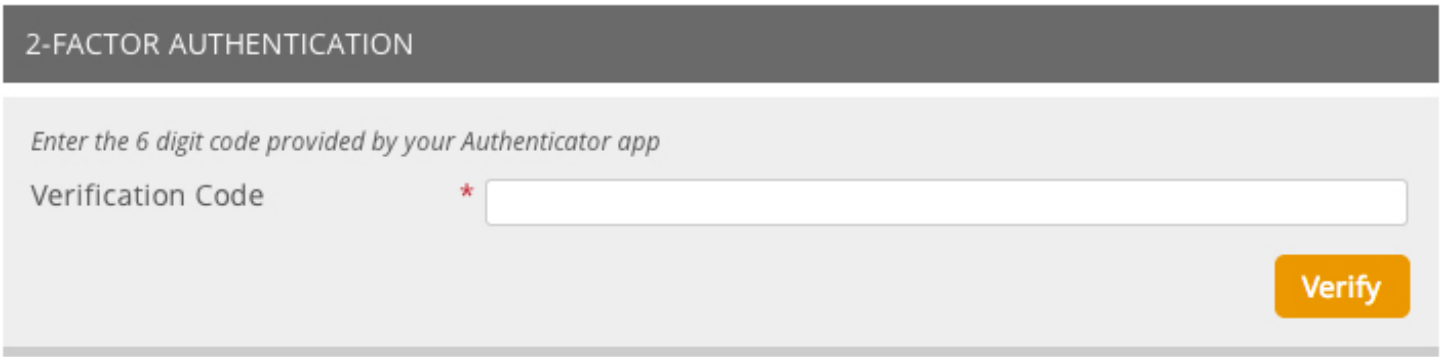


fig.1: 2-Factor Authentication Form

# Setup Instructions

1. **Download *Google Authenticator***

   The first time you reach the *VERIFY* page, you will need to **download *Google Authenticator*** on your device, and set up an account. Download and install the *Google Authenticator* app from your device's app store. Here are specific instructions:

   - **ANDROID:** If using an android device, download Google Authenticator from Google Play.
   - **IPHONE:** If using an iPhone, download the Google Authenticator application from the App store.
   - **IPAD:** If using an IPAD, search for Google Authenticator on the App store. Only one app will be shown and it is not correct, so to find Google Authenticator, change IPAD only at the top left to iPhone only. Google authenticator will then be displayed and you can download it. The iPhone version will work on IPADs.

2. **Run *Google Authenticator***

   Run Google Authenticator on your device and click **Add an Account** - this can be found as part of the initial setup process, or in the app's menu if you have used the Authenticator before.

3. **Scan the barcode**

   In order to pair your Google Autheniticator account with your COPM Web-App account, you now need to go back to the COPM Web-App VERIFY page, and **scan the barcode** on the screen into *Google Authenticator*. (If you do not have a scanner app on your device, you may also have to download a scanner app (such as Barcode Scanner), or you can manually enter the 16-digit Secret Key instead) (*see fig.2 below*).

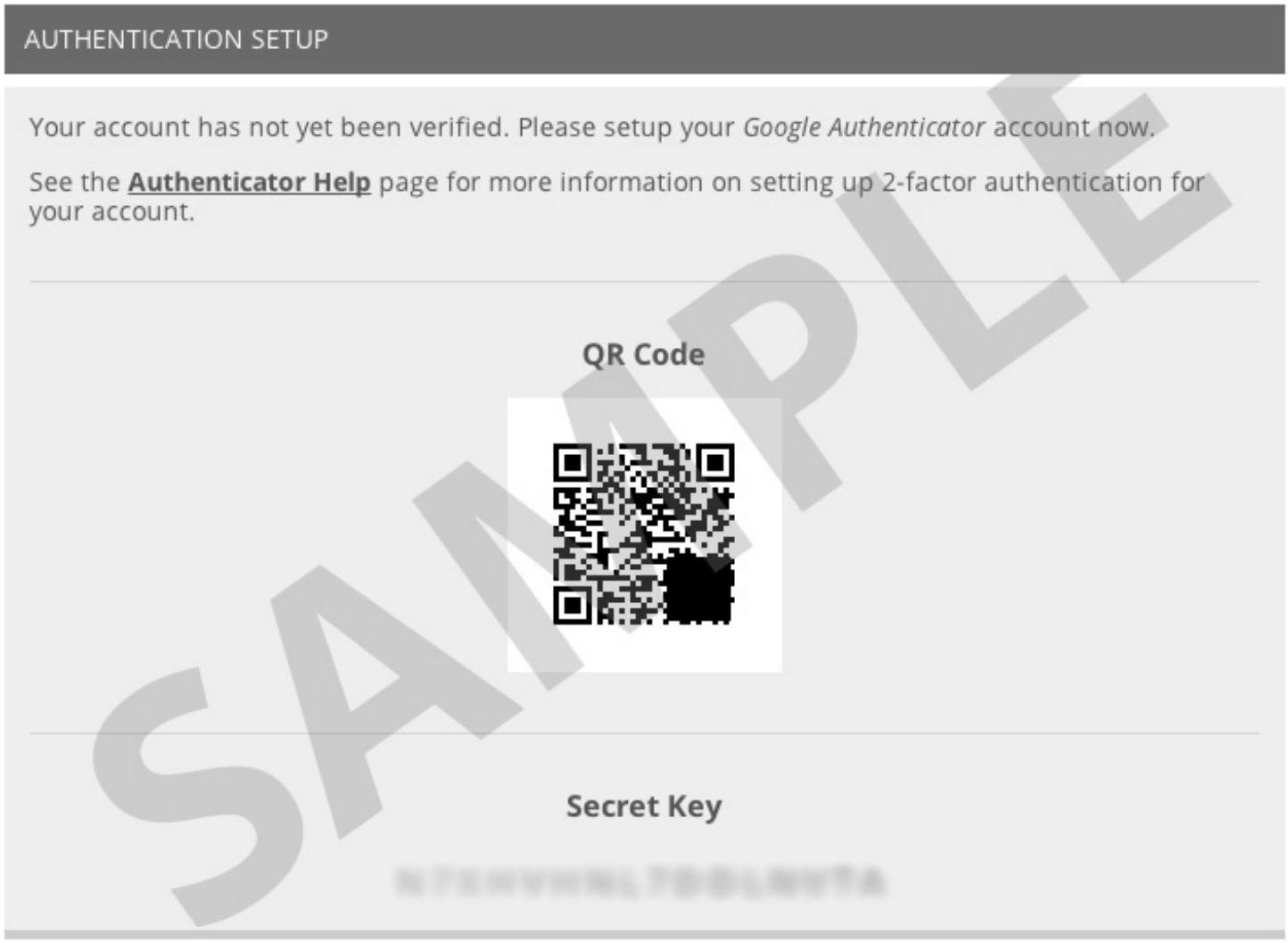

fig.2: Authentication Information

That's it! *Google Authenticator* will now show a 6-digit code that changes every 30 seconds. Enter this code on the *VERIFY* page to complete the login process. Remember you will need to check the authenticator app and enter a new verification code each time you login.

# Changing to a New Device for 2-Factor Authentication:

- When you change the device that Google Authenticator is installed on, 2-Factor Authentication needs to be turned off for your account and then reactivated for the new device. This is done to ensure the highest level of security and protection of privacy.
- COPM Inc can facilitate this change. Please email us at contact@thecopm.ca with your account user name and the email you are using for the account. Please verify that you wish to deactivate the account on your old device.
- COPM Inc will provide this information to 14theories
- 14theories will deactivate 2-Factor Authentication for your account.
- Once this has been completed, COPM Inc will contact you. You will then be able to log into your account to set up 2-Factor Authentication on your new device.

If you plan to use multiple devices simultaneously with your account, you will need to either authenticate all of them at once, or write down your secret key for later. Please be aware that anyone who obtains your secret key will also be able to set up their own device to work with your account.