Home Office

Multi-Factor Authentication

Multi-Factor Authentication

The Multi-Factor Authentication (MFA) setup is essential to the registration process. This security measure requires you to authenticate your login with an additional six-digit code, which will be prompted each time you access the portal.

This document serves as a comprehensive support guide, offering detailed instructions for the MFA setup that extend beyond the initial registration phase. While MFA is integrated into the registration, users may choose to switch between Google Authentication and Email Authentication at any point. This guide provides supplementary assistance for navigating the MFA feature throughout any stage of interaction with the product.

The most secure option is to opt-in through the Google Authenticator app. However, if you do not want to use the Google Authenticator app, you can opt-out by selecting **'Don't want to use an app?'** and proceed with verification via email.

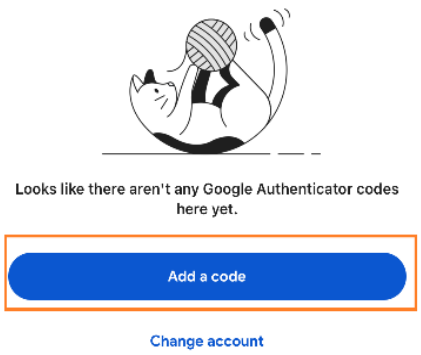
Opt-in: Google Authenticator app

If you select the Multi-Factor Authentication opt-in option, you must have the Google or Microsoft Authenticator app on your device.

To set up the Multi-Factor Authentication on your device, please follow the steps below:

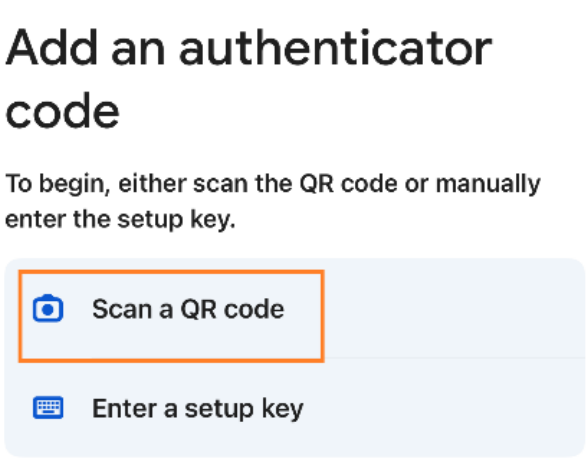
Scan a QR Code

1. Download the **Google or Microsoft Authenticator app** from your mobile device app store.
2. Open the **Google or Microsoft Authenticator app.**

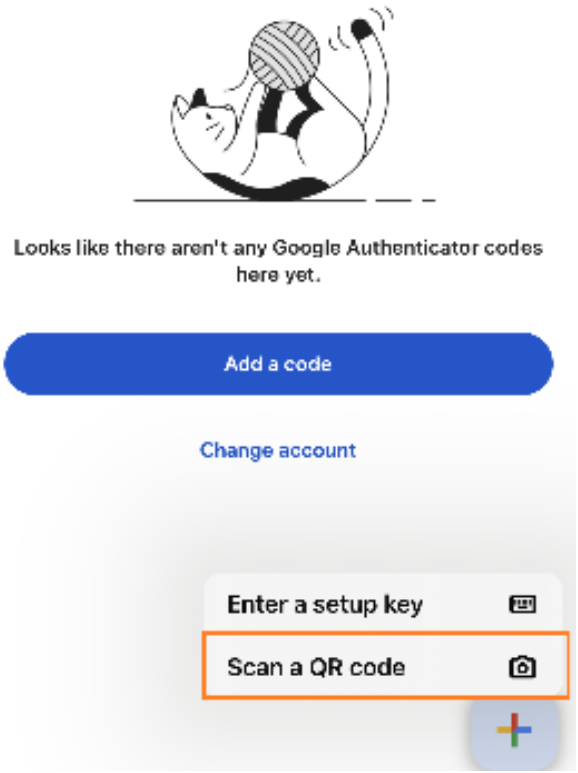


3. Select the **Add a code** or the **Plus** button.

Add a Code - Page

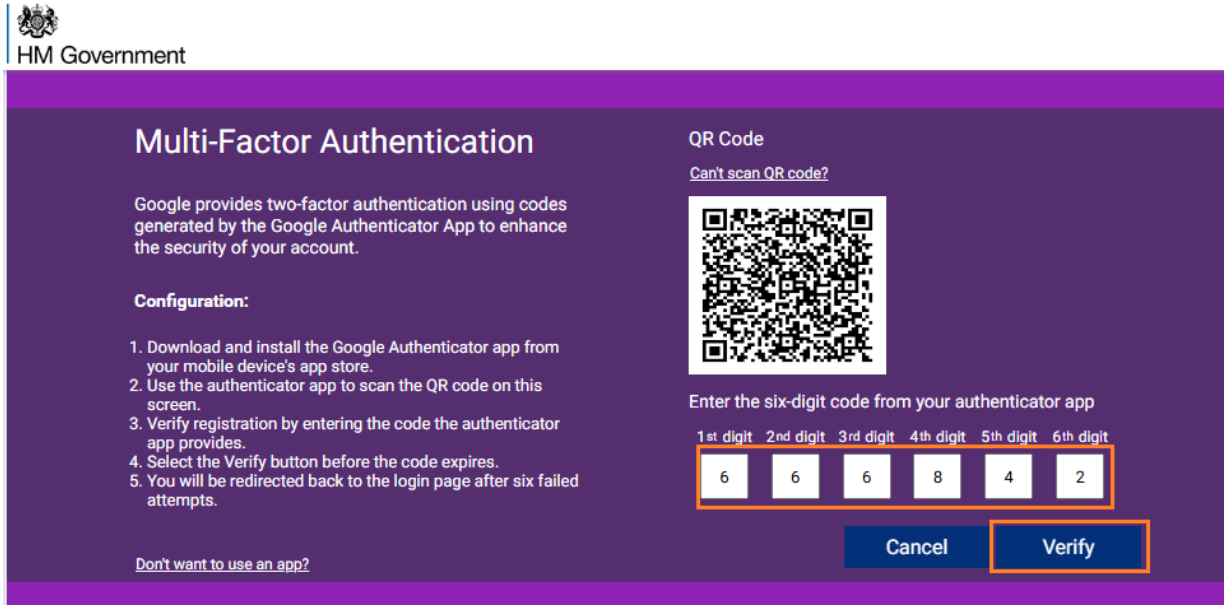


Plus button - Page



4. Select **Scan a QR code**.
5. The **scanner box** will appear, and then you must scan the QR Code on the Multi-Factor Authentication page. A **verification code** will appear in the Google Authenticator app.

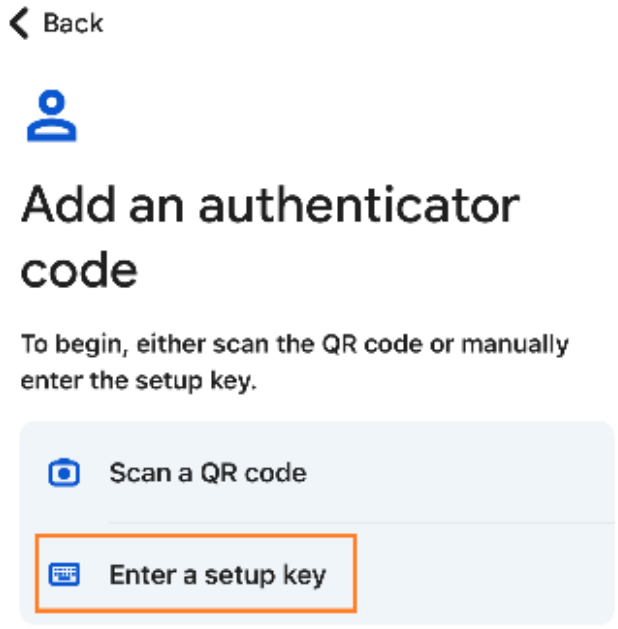
6. Enter the **verification code** on the portal's **Multi-Factor Authentication** page and select **Verify** before the code expires on the App.



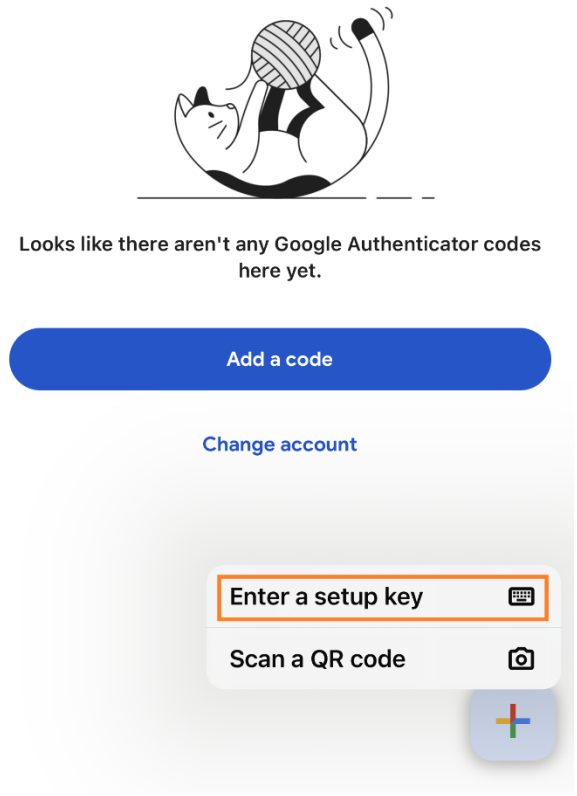
Enter a set-up key (If you can't scan the QR code)

1. Download the **Google or Microsoft Authenticator app** from your mobile device app store.
2. Open the **Google or Microsoft Authenticator app**
3. Click on the **Add a code** or the **Plus** button.

Add a Code - Page

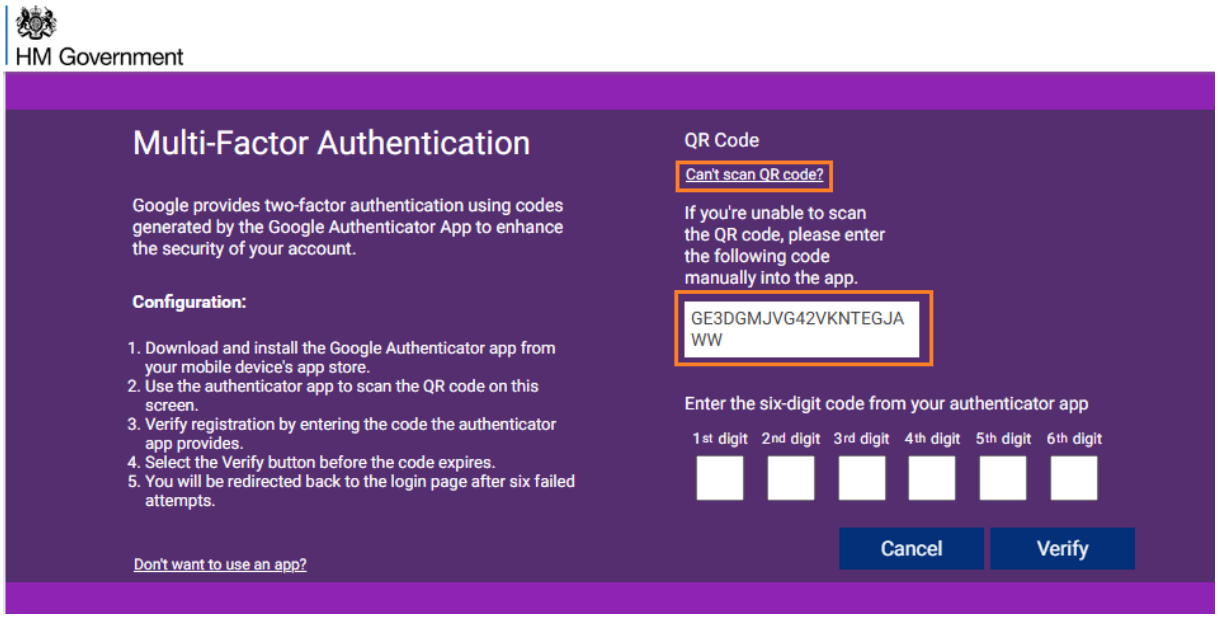


Plus button - Page

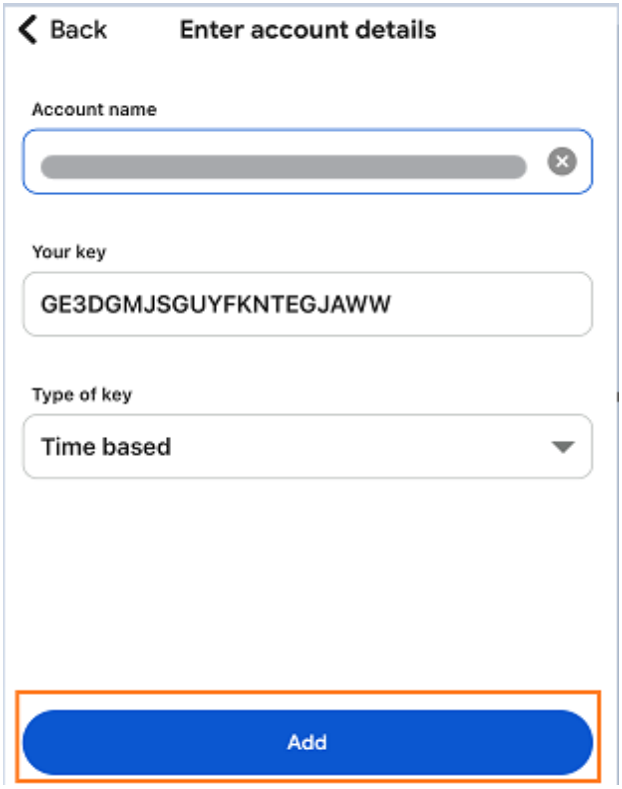


4. Select **Enter a setup key.**
5. Enter account details as follows:

a. **Account name:** Registered email address.
b. **Your key:** You obtain the key from the MFA page by selecting **Can't scan QR code?** which will generate the key.

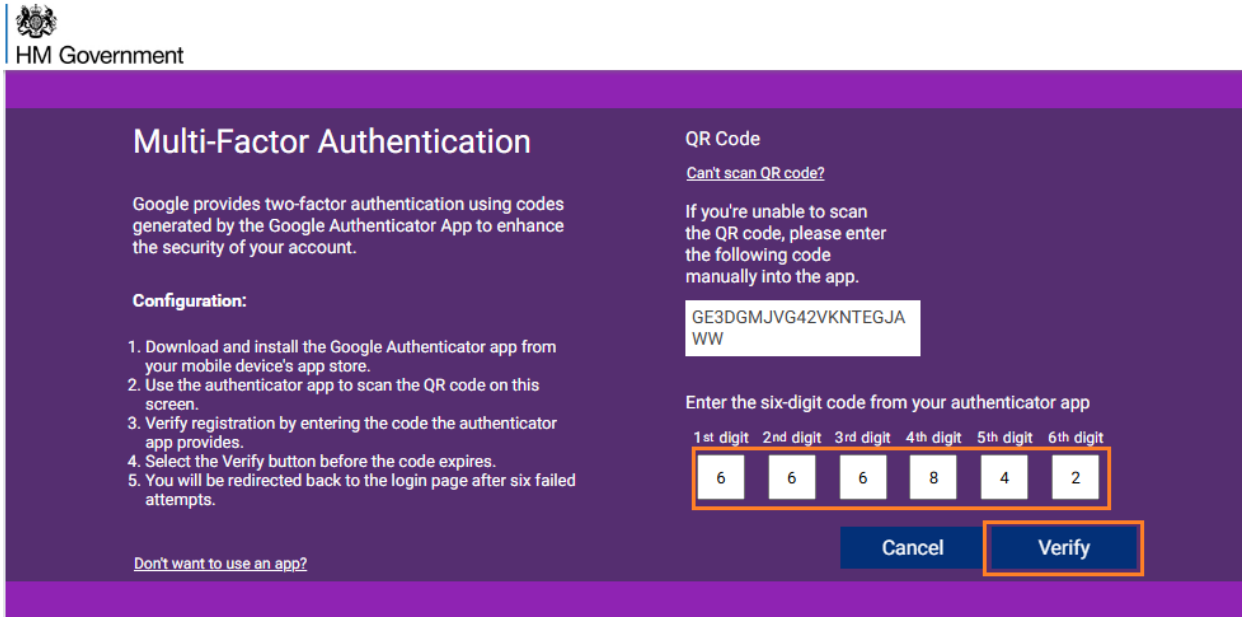


c. **Type of key:** Select **Time based**



6. When you've filled in the account details, select Add. A **verification code** will appear in the Google or Microsoft Authenticator app.

7. Enter the **verification code** on the portal's **Multi-Factor Authentication** page and select **Verify** before the code expires on the app.



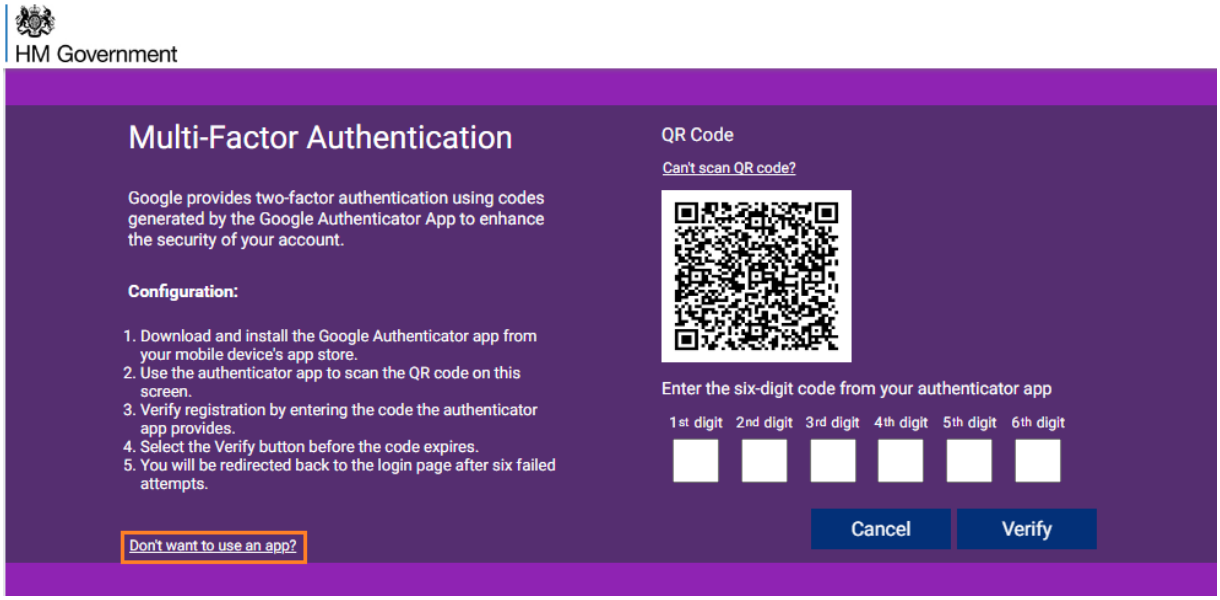
Once you have completed each step, you will be set up on the Google or Microsoft Authenticator app and redirected to the portal homepage.

Additional Information
Scanning the QR code without downloading the app will redirect you to your device's password settings - this will not set up MFA and ultimately will not allow you entry into the portal.

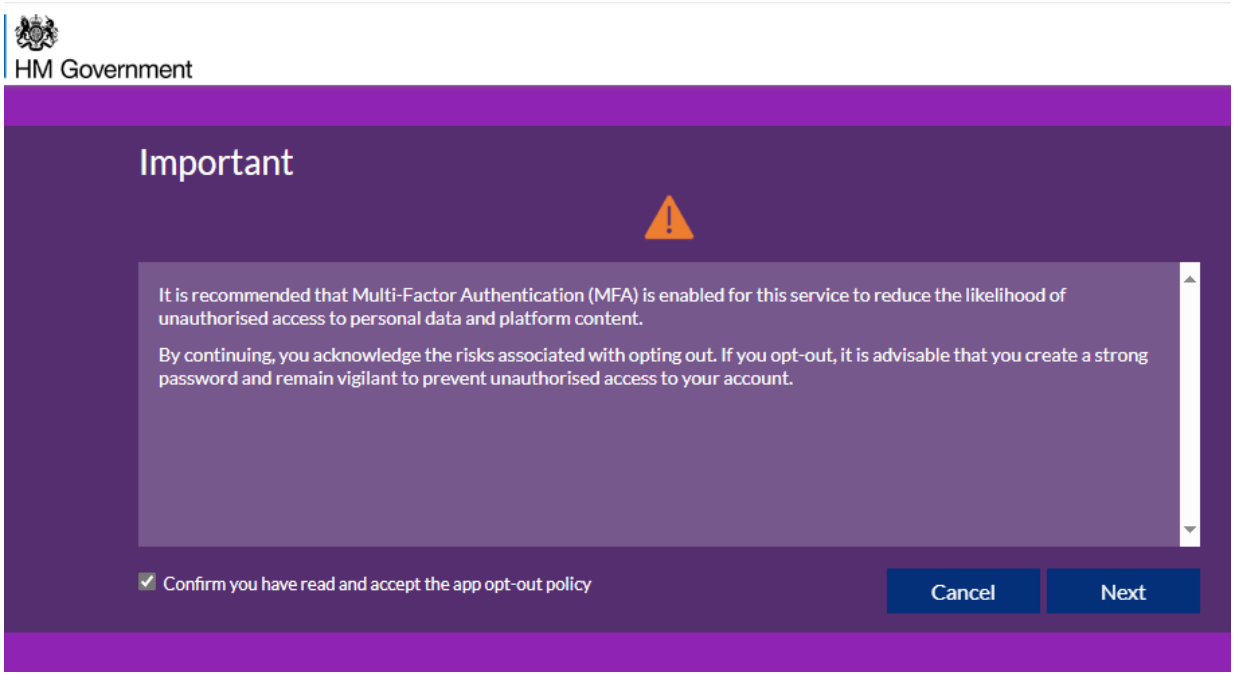
Opt-out: Email

If you select the Multi-Factor Authentication opt-out option, you will receive your six-digit code via email.

To set up the Multi-Factor Authentication to your email, please follow the steps below:
1. Select **Don't want to use an app?**

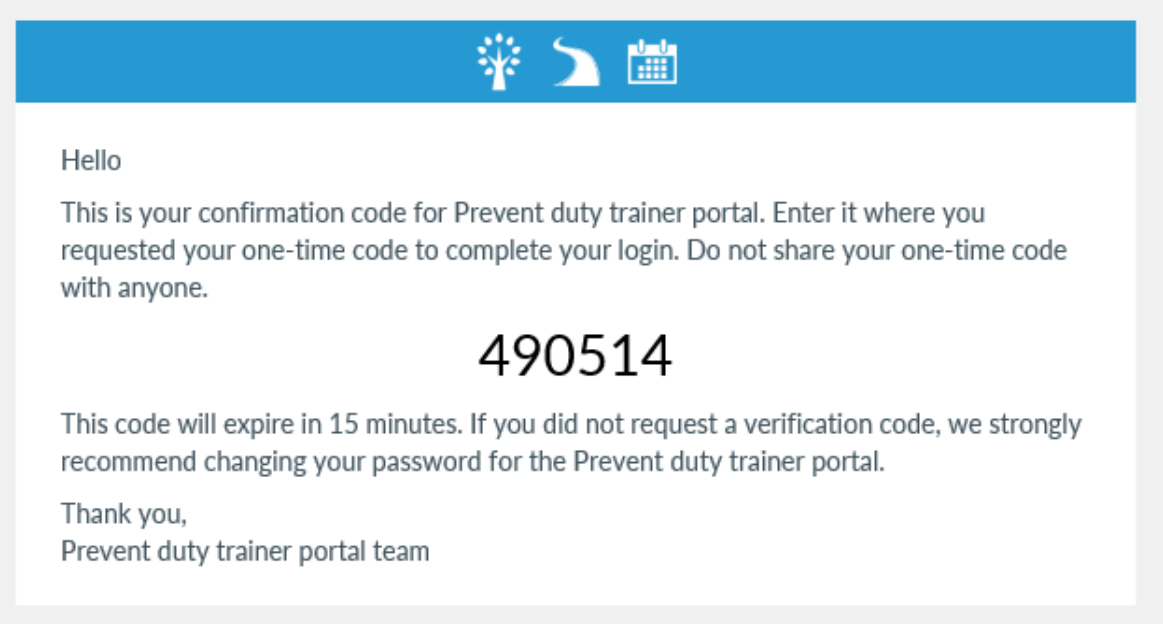


2. **Read and accept** the app Opt-out policy.

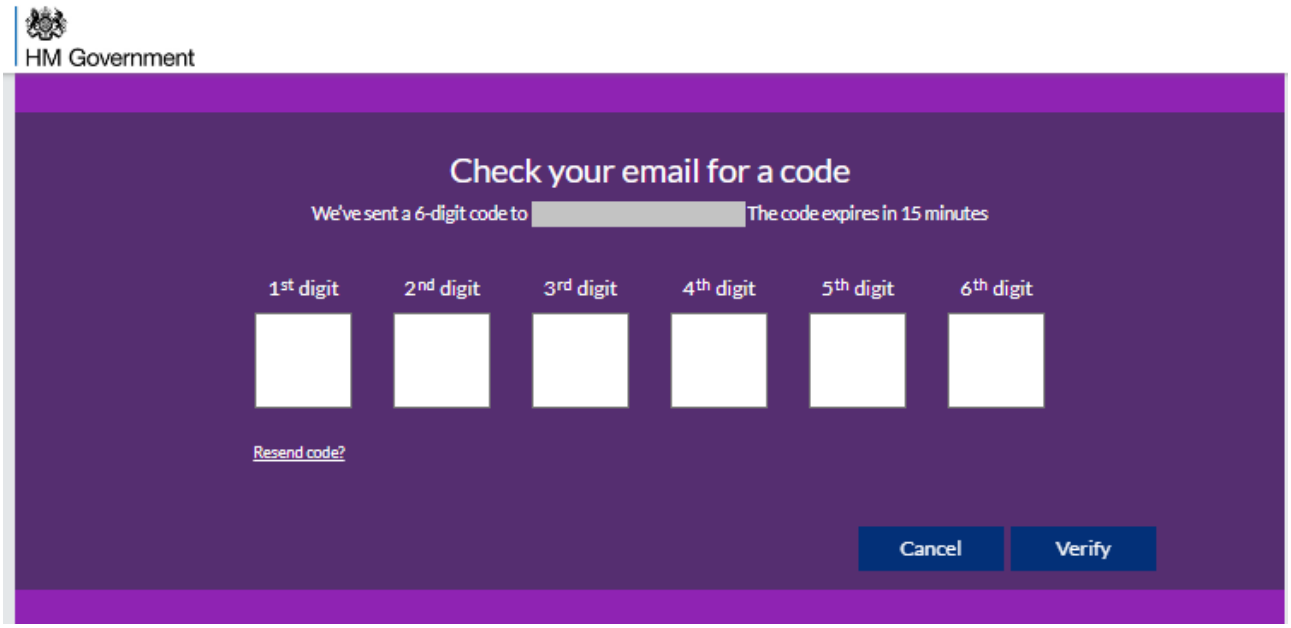


3. Wait for the digit code to be sent to your email from noreply@prevent-trainer-portal.homeoffice.gov.uk. This can take a few minutes to arrive.

4. Check your inbox for the verification code. If the email has not arrived, please check your 'Junk' or 'Spam' folder.



5. Enter the verification code on the portal's **Multi-Factor Authentication** page and select **Verify** before the code expires.



Once you have completed each step, your email will be set up for MFA and you'll be redirected to the portal's homepage.