



Office Message Encryption (OME)

**Step-by-step guide on how to open a secure,
encrypted email sent from Birmingham City Council
and Birmingham Children's Trust**

Introduction

From the beginning of September 2020, Birmingham City Council and Birmingham Children's Trust will start using **Microsoft's Office Message Encryption (OME)** process for sending sensitive information via encrypted (secure) emails, including documents holding sensitive information and large document files.

As this new process works with other Microsoft Office 365 tools that the council already uses, email encryption and sharing documents will become much easier and more secure.

- **Accessing encrypted emails**- to decrypt the email message, you will firstly need to follow a one-time passcode activation process. More information about this process and how to decrypt and open a secure email is explained in this easy to follow step-by-step guide.
- **Recognising genuine encrypted emails** - we will only ever contact you from a Birmingham City Council email address ending "@birmingham.gov.uk" or a Birmingham Children's Trust email address ending '@birminghamchildrenstrust.co.uk'.

Instructions

1. When you open the email from your inbox, you will see the following message. Click **'Read the Message'**. **Please note** - an encrypted email message will expire within 90 day from when it is originally sent.

From Birmingham City Council



From Birmingham Children's Trust



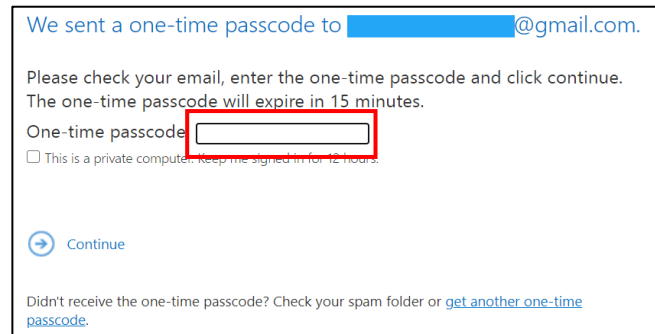
2. If the 90-day period has expired, you will receive the following error message: **'The message you're trying to view expired on M/D/YYYY at HH:MM AM/PM and can't be viewed'**.

The message you're trying to view expired on 7/18/2020 at 11:36 AM and can't be viewed.

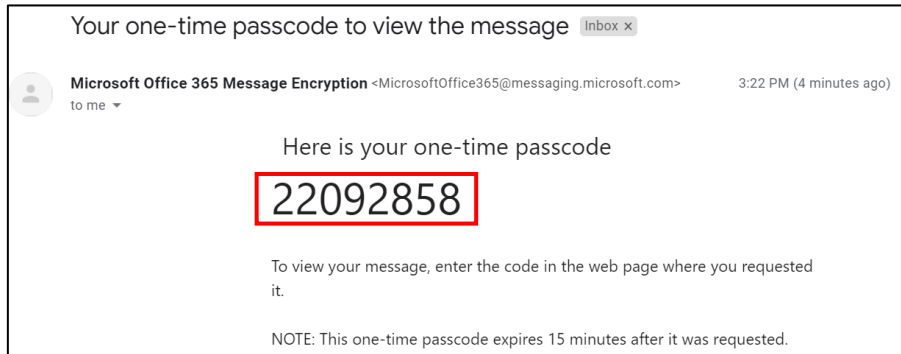
3. If you open the email within the 90-day period (since the email was originally sent), the following message will appear. Click on **‘Sign in with a One-time passcode’**.



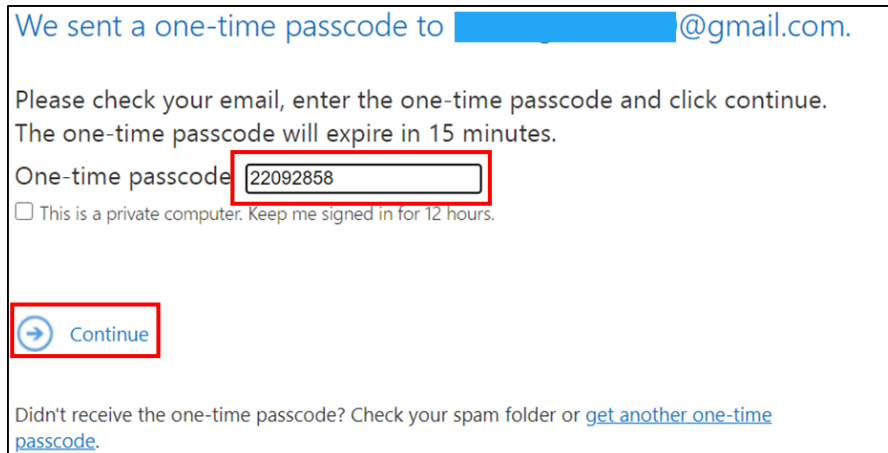
4. You will next see a verification page with a box for a one-time passcode. An email will be sent to you with an **8-digit passcode**.



5. Check your Inbox or Spam folder for the email with the **one-time passcode**.



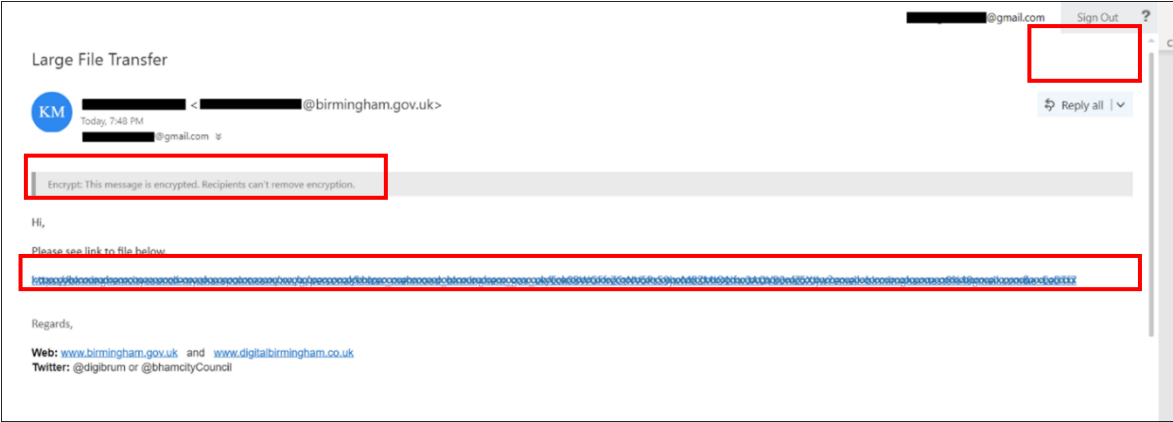
6. Enter the passcode and press **'Continue'**



7. You will now be able to read the message.

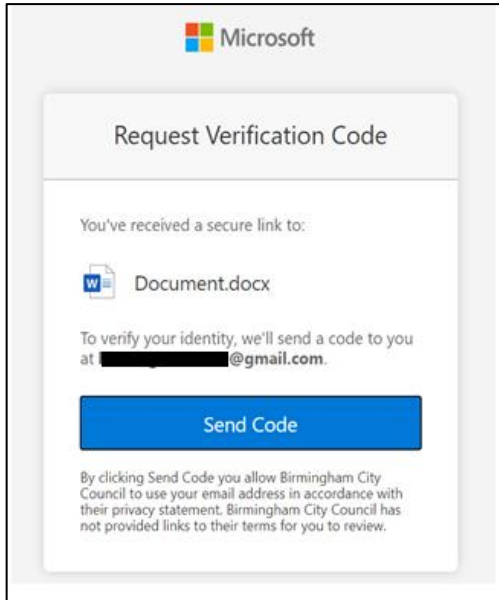
Please note that if you **'reply'** or **'forward'** the email, it will remain encrypted. This is because the encryption has been set by the email sender and cannot be changed by any email recipient. So, you cannot send a reply or forward the email message without the encryption remaining in place.

8. You may also receive an email including a link for a large file that has been shared with you. To open the file, firstly click on this link.

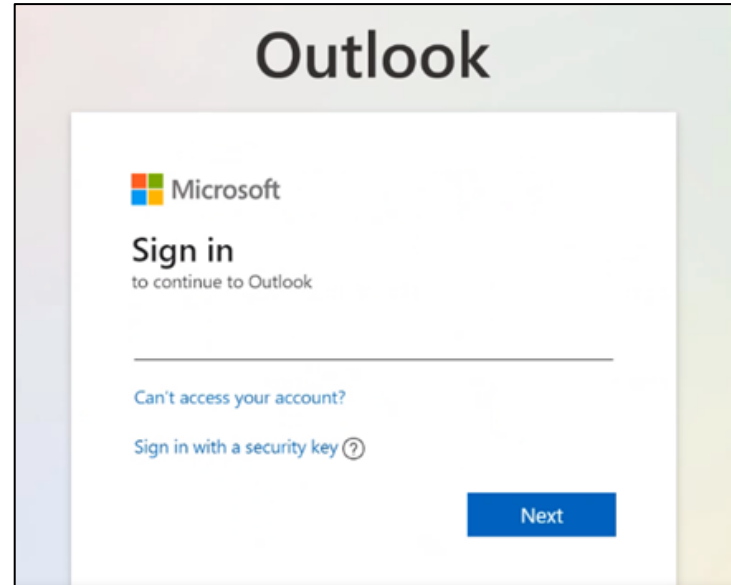


9. When you click on the large file link in the email, you will either see a 'verification box' appear or be 'prompted to login'. If a verification box appears, proceed to **step 10**. If you are prompted to login, proceed to **step 12**

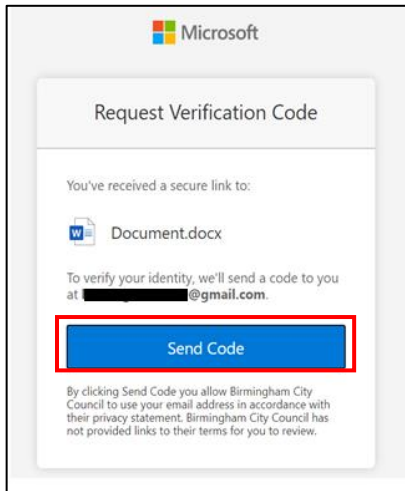
Verification box



prompted to login

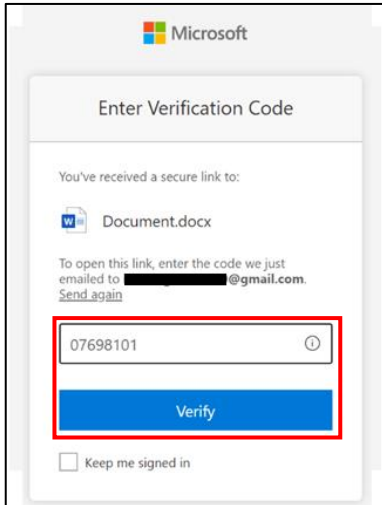


10. Click **'Send Code'** to trigger an email with an 8-digit passcode. As you are the recipient of the initial email, the email containing the passcode will be sent direct to you.

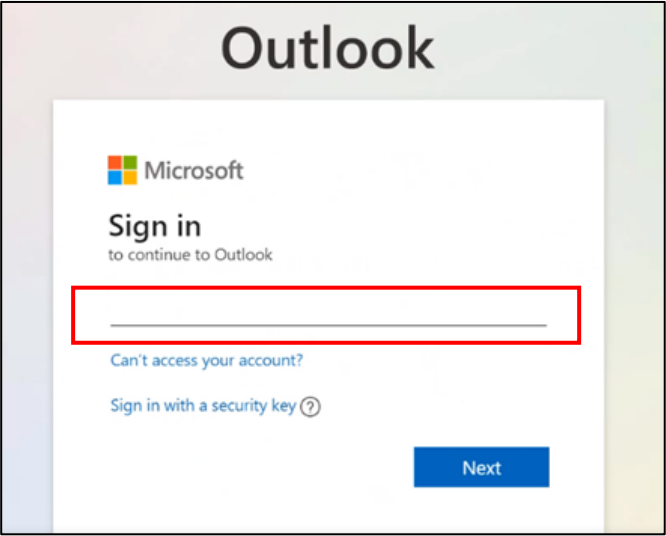


Note: if the link is shared with another person, they **WILL NOT** be able to access the file as they are not authorised to do so by Birmingham City Council/ Birmingham Children's Trust.

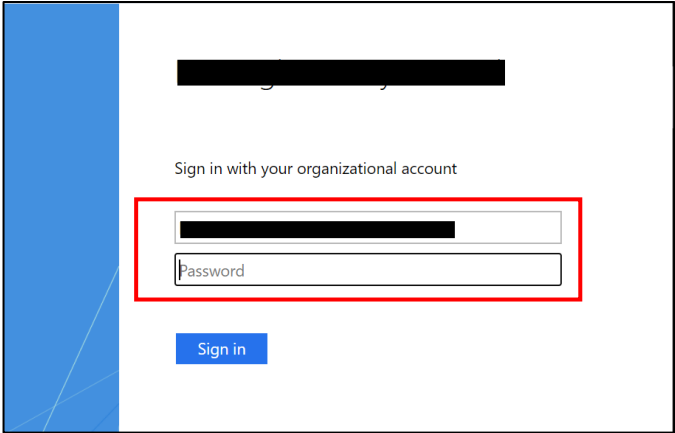
11. Check your Inbox and Spam folder for the email with the 8-digit passcode.
Enter the code in the box and click **'Verify'** and proceed to **step 14**.



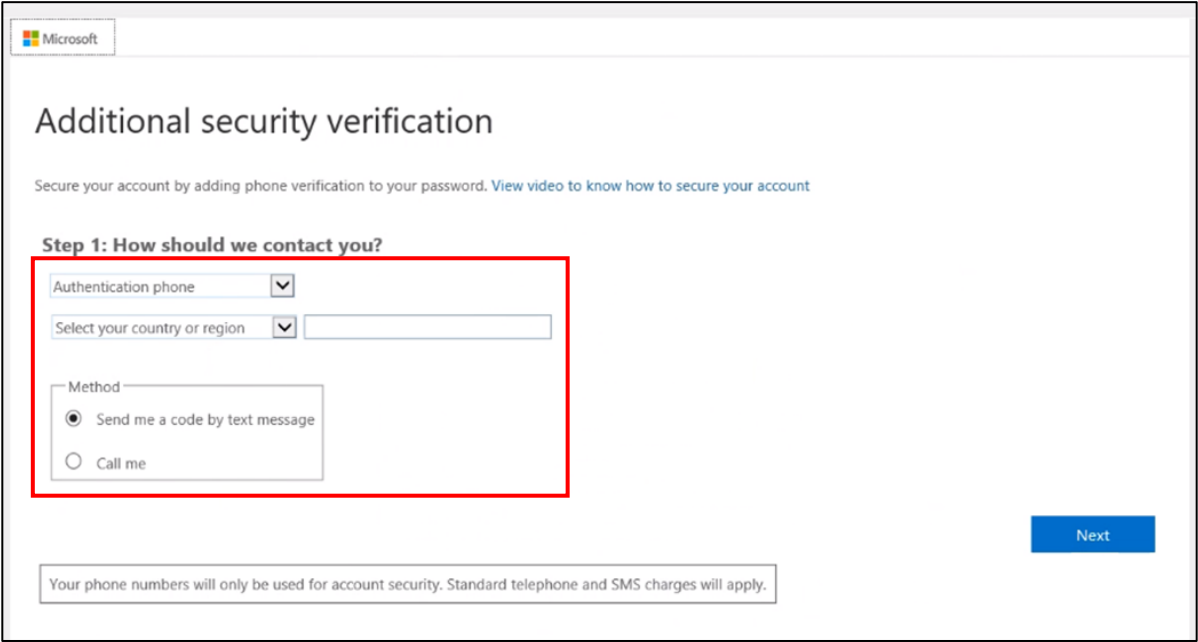
12. Enter your email address and press **'Next'**



13. Sign in using your office365 email and password.
Click **'Sign in'**



NOTE: If you are prompted to authenticate using multi factor authentication, then please follow the on screen instructions, and choose your preferred method.



The screenshot shows a Microsoft account security verification page. At the top left is the Microsoft logo. The main heading is "Additional security verification". Below it, a sub-heading reads "Secure your account by adding phone verification to your password. View video to know how to secure your account". The primary instruction is "Step 1: How should we contact you?". This section contains three input fields: "Authentication phone" (a dropdown menu), "Select your country or region" (a dropdown menu with an adjacent text box), and "Method" (a group box containing two radio button options: "Send me a code by text message" (which is selected) and "Call me"). A blue "Next" button is positioned to the right of the form. At the bottom, a disclaimer states: "Your phone numbers will only be used for account security. Standard telephone and SMS charges will apply."

14. You will now be able to access the file.

