



# LOMBARD

## Guide to Accessing Secure Email

### Secure emails from Lombard Bank

The purpose of these guidelines is to provide information regarding the manner in which emails secured by encryption originating from Lombard Bank may be viewed and read by recipients. Encryption is intended to minimise the risk of unauthorised access to the information contained in email communication, thereby protecting such information against misuse and / or modification.

Not all Lombard Bank emails will be encrypted – only those emails deemed to contain sensitive and / or confidential information will be encrypted. Though accessing an encrypted email will normally require additional actions by recipients, the process is not difficult to carry out.

### Outlook Message Encryption

Lombard Bank uses Microsoft Outlook tools to encrypt emails. The actions needed to be taken by a recipient depend on the type of email service used.

1. *Recipients making use of a Microsoft service to read emails e.g., Microsoft Outlook 365 or Microsoft Outlook on the web (OWA).*

Such recipients will access the email seamlessly, without any further action.

2. *Other recipients*

An encrypted email opened by other recipients (those not making use of a Microsoft service) will look as shown in figure 1. To proceed to open and read the encrypted email, the recipient will need to click on the link labelled 'Read the message'.

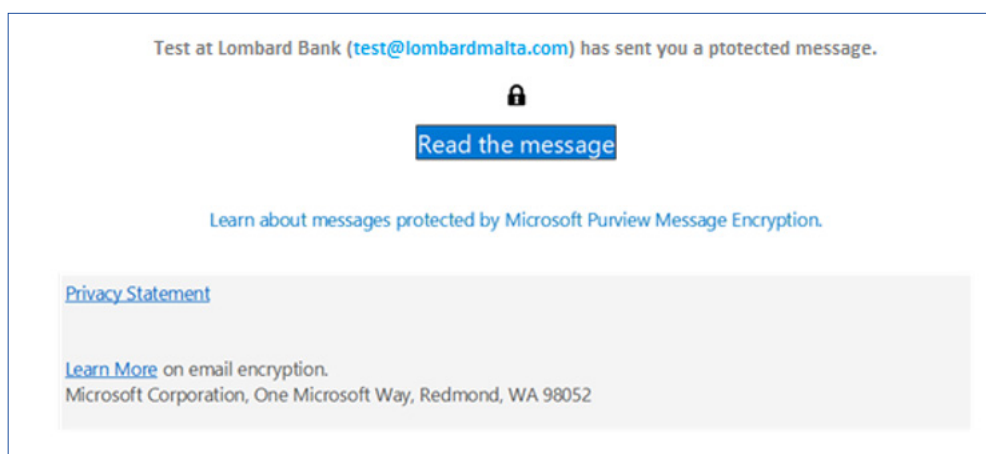


Figure 1 - Opening an encrypted email.

Clicking on 'Read the message' will display the options shown in figure 2.

To proceed to open the secure email recipient may select either of the two options presented: using the credentials of the email account used to read the encrypted email e.g., Gmail, Yahoo Mail, etc or requesting a one-time passcode.

If recipient chooses to sign in the email account, sharing of email account credentials with Office365 will need to be approved.

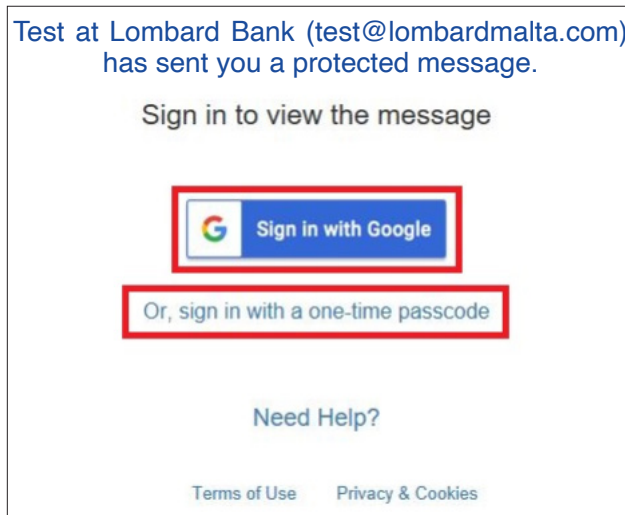
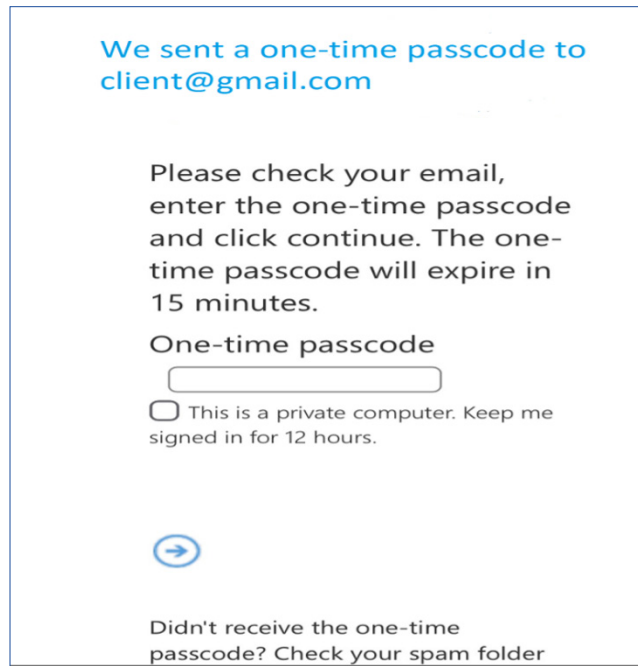


Figure 2 - Options displayed on clicking 'Read the message.'

If recipient chooses to read the message using a one-time passcode, redirection to a page to enter the single-use code provided will be required, as in Figure 3.




We sent a one-time passcode to client@gmail.com

Please check your email, enter the one-time passcode and click continue. The one-time passcode will expire in 15 minutes.

One-time passcode

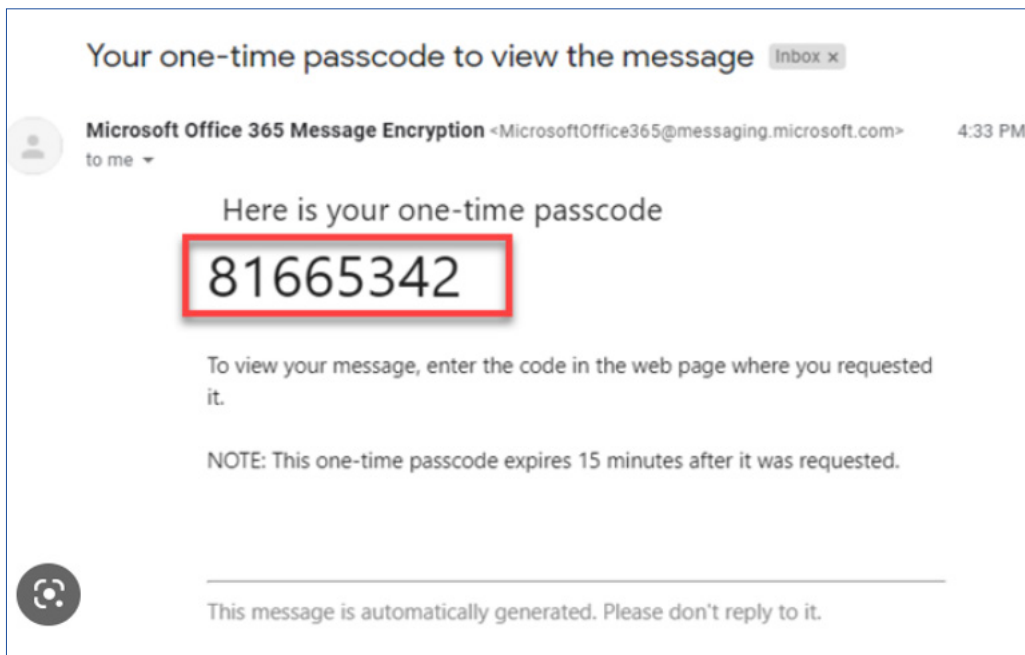
This is a private computer. Keep me signed in for 12 hours.




Didn't receive the one-time passcode? Check your spam folder

Figure 3 - Redirected page to insert 'One-time Passcode'.

In addition, the one-time passcode is sent in a separate email (Figure 4). The recipient must copy the pin code provided to the appropriate box on the redirected page as shown in Figure 3. Should the one-time passcode email appear not to have been received, recipient should check the spam folder, in the event that the email would have been redirected there.



Your one-time passcode to view the message Inbox x


 **Microsoft Office 365 Message Encryption** <MicrosoftOffice365@messaging.microsoft.com> 4:33 PM  
to me ▾

Here is your one-time passcode

**81665342**

To view your message, enter the code in the web page where you requested it.

NOTE: This one-time passcode expires 15 minutes after it was requested.



This message is automatically generated. Please don't reply to it.

Figure 4 - Email received when selecting 'One-time Passcode'.