



## **Guidance for recipients of Secure Email Messages from Lloyds Banking Group**

### **Introduction**

You have been sent this document as your Lloyds Banking Group contact is sending confidential information to you via email and our policy is to ensure that confidential information is kept secure and that it is only read by those it is addressed to.

This document provides an overview of the secure mail service used by Lloyds Banking Group. Whilst email provides a quick and convenient way of sending and receiving information, messages transmitted over the internet are not secure. Sending a message using email can be likened to sending a postcard in the post – anyone handling the postcard whilst it is being delivered can read what's on it. In order to ensure that confidential information contained in emails remains private, Lloyds Banking Group uses a secure mail product based on Symantec's Encryption Management Servers. This service encrypts and decrypts email messages and their attachments preventing the contents from being seen by anyone other than the addressee. The recipient does not need to be a Symantec Encryption user as the message can be displayed from a web browser connected to the internet.

You will receive links to your encrypted messages in your normal email client and you will be able to view and respond to them using your default browser. When you have received an encrypted message, you can reply to it, attaching files if necessary, the message and any attachments will be encrypted as well.

Please note that your secure mailbox will be deleted after 30 days if it is not accessed so it is important to ensure that you save any important documents in another location as they will be deleted after this period has elapsed; please do not assume that this mailbox is a permanent repository for your data

### **Pre-requisites**

In order to use this service you will need:

- an email client that will display https content;
- a web browser with connection to the internet;
- emails from lloydsbanking.com to be white-listed on any spam filters, either within your email/webmail client or by your ISP.

To ensure you can contact the Symantec Secure Mail servers please click here

<https://securemail.lloydsbanking.com>

You should see a screen similar to the following displayed in your browser.



**LLOYDS BANKING GROUP**

**Symantec.**

**Welcome to Symantec Web Email Protection**

In order to gain access to your account and messages you must first enter your email and passphrase associated with this account.

**Please enter your passphrase:**

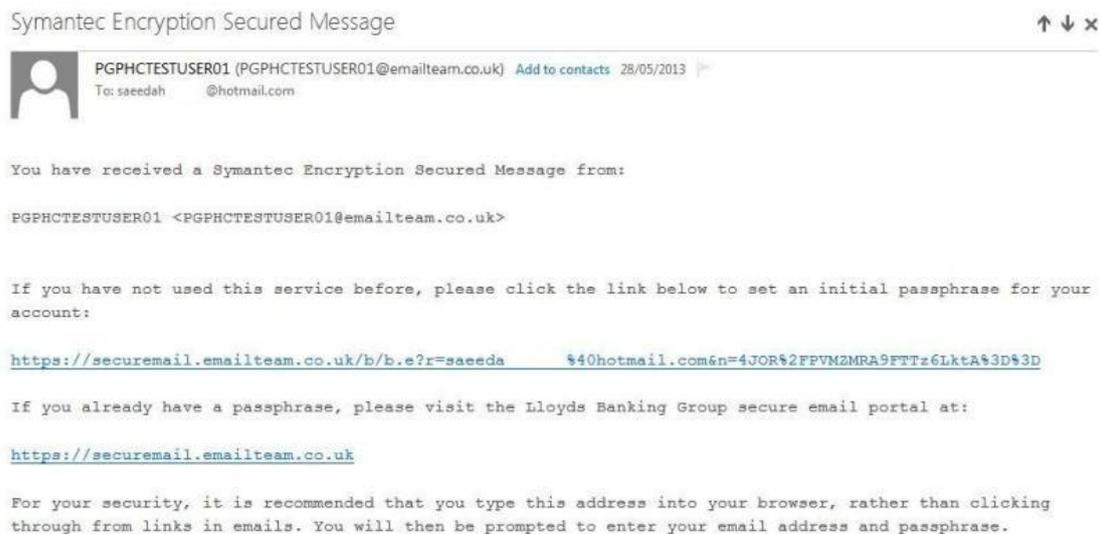
Passphrase:

[I lost my passphrase](#)

Copyright © 2011 Symantec Corporation. All Rights Reserved.

## User Guide

If you have not communicated via LBG Symantec Web Email you will need to click on the 1<sup>st</sup> link in your message mail and you can set up your account



Symantec Encryption Secured Message ↑ ↓ ×

 PGPHCTESTUSER01 (PGPHCTESTUSER01@emailteam.co.uk) [Add to contacts](#) 28/05/2013  
To: saeedah @hotmail.com

You have received a Symantec Encryption Secured Message from:

PGPHCTESTUSER01 <PGPHCTESTUSER01@emailteam.co.uk>

If you have not used this service before, please click the link below to set an initial passphrase for your account:

<https://securemail.emailteam.co.uk/b/b.e?r=saeeda %40hotmail.com&n=4JOR%2FPVM2MRA9FTTz6LktA%3D%3D>

If you already have a passphrase, please visit the Lloyds Banking Group secure email portal at:

<https://securemail.emailteam.co.uk>

For your security, it is recommended that you type this address into your browser, rather than clicking through from links in emails. You will then be prompted to enter your email address and passphrase.

The following screen will be shown



**You have received an encrypted message**

Please create a passphrase to secure future messages delivered to you.

This server requires your passphrase to meet the following requirements:

- They must be at least 8 characters long.
- It must include an uppercase letter, a lowercase letter, a digit and a punctuation mark.

For example, "kittycat" is not a valid passphrase, but "k1ttYc@t" is a valid passphrase.

Here are some recommendations for protecting your passphrase:

- Use an easy to remember passphrase that you don't need to write down.
- Don't use obvious passphrases that can be easily guessed.
- Don't make your passphrase a single word.
- Don't use famous quotations.

Passphrase:

Confirm Passphrase:

[Continue](#)

Please set yourself up with a **secure** passphrase and then return to your email message and use the second link.

The following screen will be displayed (the passphrase that you created will need to be entered here).



**Welcome to Symantec Web Email Protection**

In order to gain access to your account and messages you must first enter your email and passphrase associated with this account.

Please enter your passphrase:

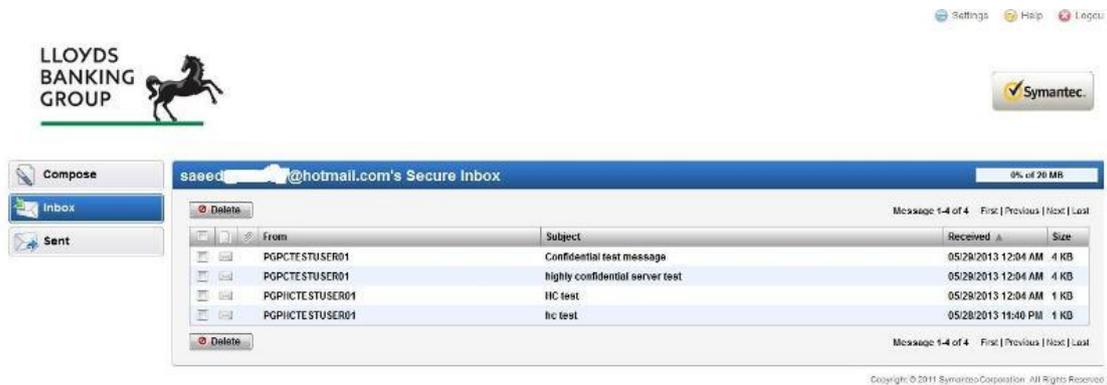
Passphrase:

[I lost my passphrase](#)

[Login](#)

Copyright © 2011 Symantec Corporation. All Rights Reserved.

Click the Login Button: The Symantec Web Email inbox screen will be displayed.  
Any emails sent to you from LBG will be displayed here



You can then open the email.

Clicking on the Compose button will allow you to create & send a secure email to any LBG user who has Symantec Email Encryption.



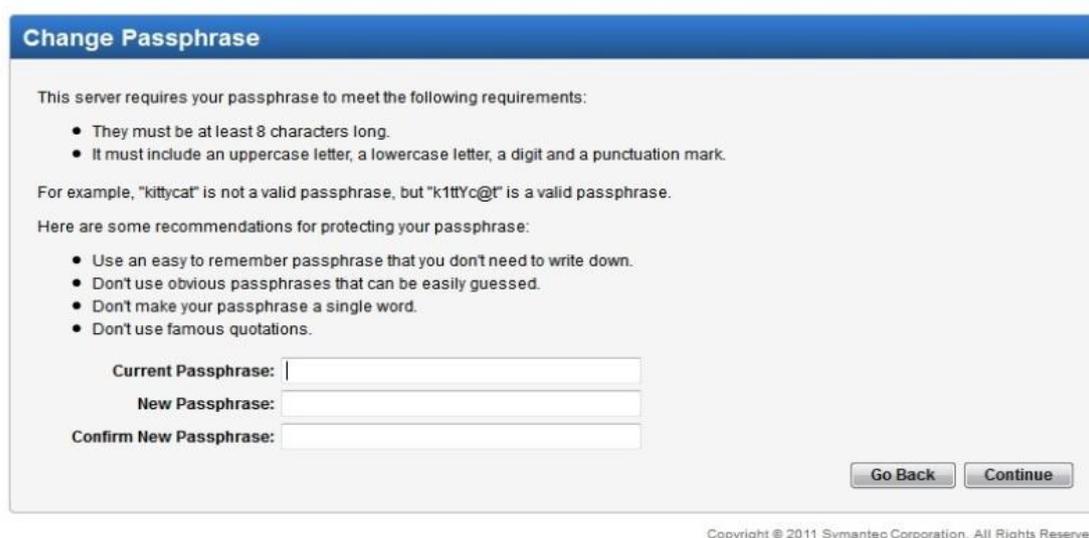
**Message Sent**  
Your message was sent.



The Sent button will display any emails that have been sent using this facility.



The settings button will allow the passphrase to be changed



Please note that this mailbox will be deleted after 30 days if it is not accessed. Please ensure that you save any important documents in another location as they will be deleted after 30 days; please do not assume that this mailbox is a permanent repository for your data

For more detail about the Symantec product please follow this link

[http://www.symantec.com/content/en/us/enterprise/fact\\_sheets/b-encryption-management-server.pdf](http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-encryption-management-server.pdf)