VIRTRU GUIDE FOR SECURE MESSAGE RECIPIENTS

MAY 29, 2018

LONDON & COLONIAL
INNOVATION IN PENSIONS
PART OF STM GROUP PLC

VIRTRU GUIDE
FOR SECURE MESSAGE RECIPIENTS

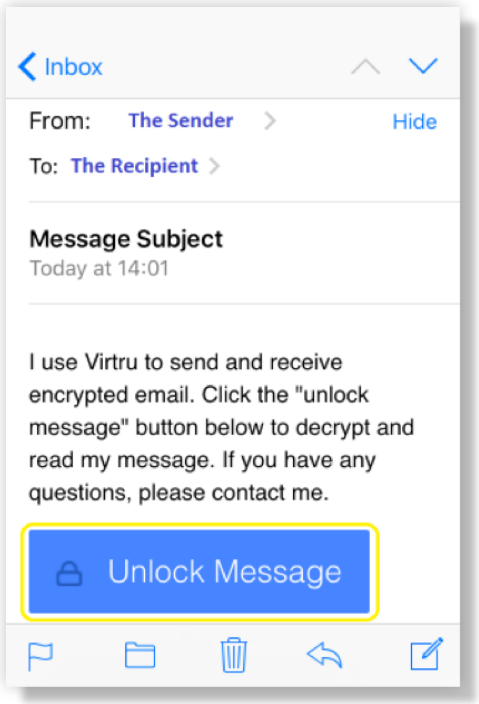
OVERVIEW

This guide explains how to read a secure email from London & Colonial which has been encrypted for secure transmission using the **Virtru** Platform.

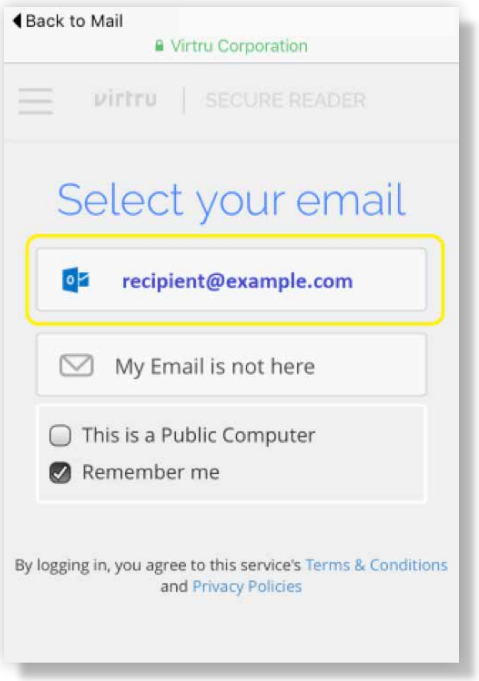
Please note that images included in this document are for illustrative purposes as the look and feel may vary on different systems.

PROCESS

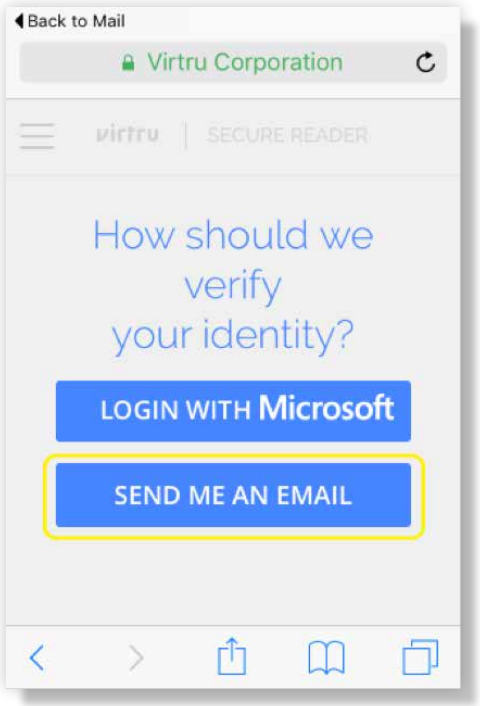
1. **Unlock Message:** Click the blue 'Unlock Message' button in the secure email to load the **Virtru Secure Reader** app in the default web browser on the device to access the protected content.

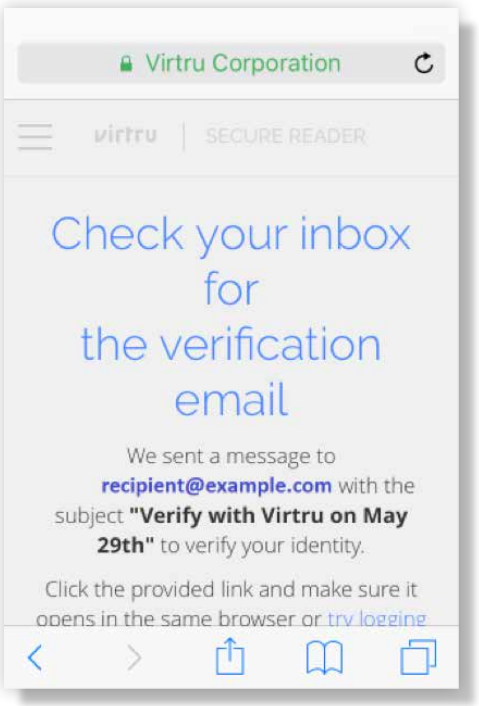


2. **Select your email:** Select your email address from the list of authorised recipients of the secure email. If you don't see yours listed, click 'My Email is not here' and enter your information.

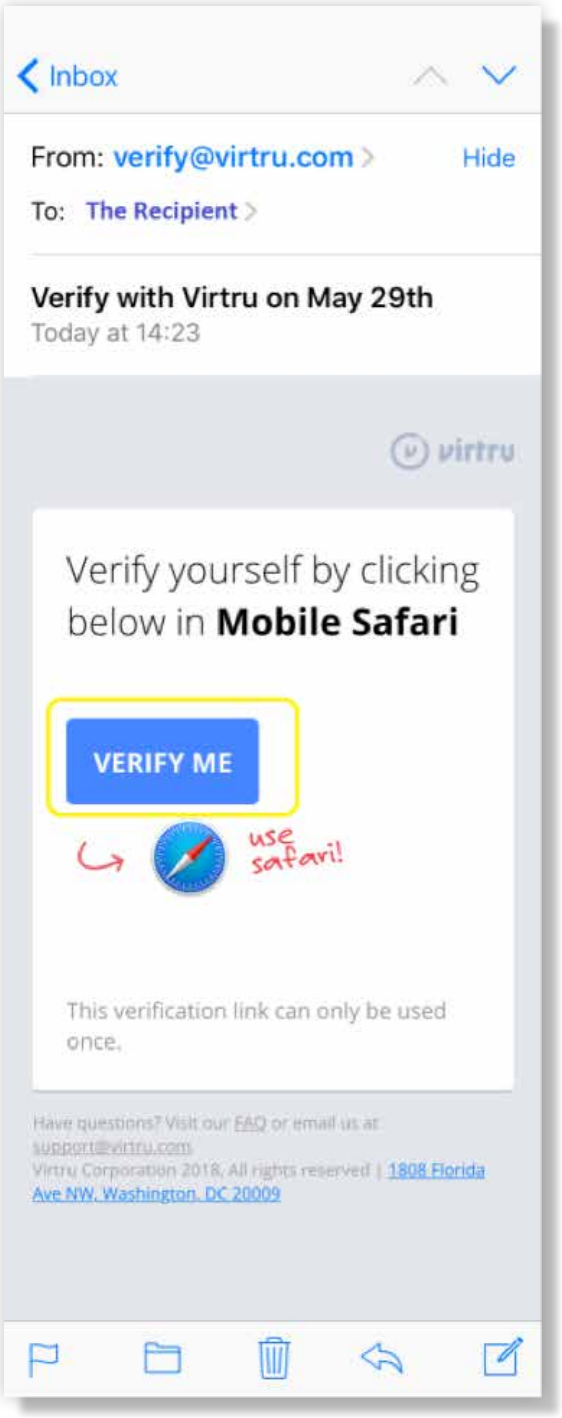


3. **Choose how to verify your identity:** You can choose 'LOGIN WITH MICROSOFT' or 'LOGIN WITH GOOGLE' if available, otherwise choose 'SEND ME AN EMAIL' and upon confirmation check the inbox of the given address for the verification email containing the 'Verify Me' link.

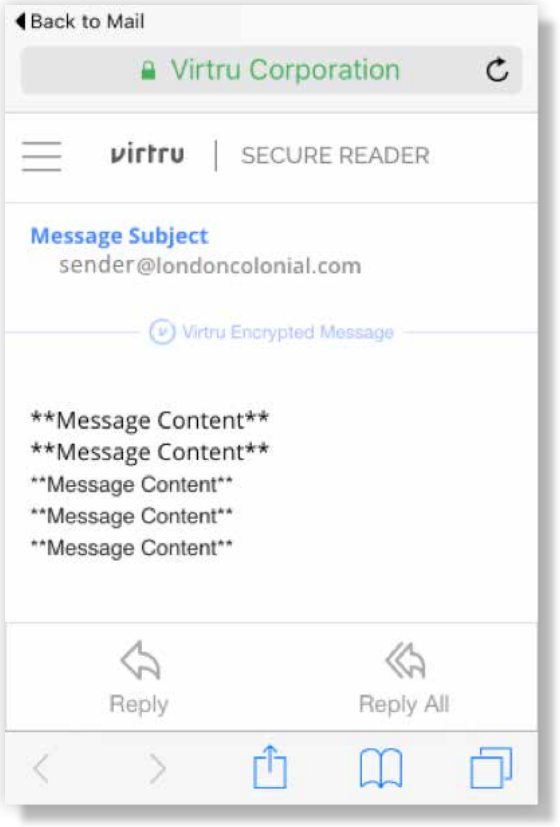




4. **Verify your email address:** Select 'VERIFY ME' to complete the authentication process for the email address.



5. **View the decrypted message:** The browser will open the link and decrypt the protected message content for viewing. The ability to decrypt further messages secured with Virtru will be saved in the browser's cache.



VIRTRU GUIDE
FOR SECURE MESSAGE RECIPIENTS

APPENDIX I - LONDON & COLONIAL USES VIRTRU

Why use the Virtru Platform?

1. **Flexibility:** Virtru allows authorised parties to receive and decrypt protected content without installing Virtru's software.
2. **Authentication:** To access protected content, recipients must authenticate with the Virtru Platform. To do this, they use their existing email credentials, rather than having to establish new usernames or passwords.
3. **Integration:** Virtru has plugins for secure client-side sharing from Microsoft Outlook desktop, OWA for Office 365, and Gmail. Recipients who don't use any of these platforms can access Virtru's Secure Reader from their browsers, so they can consume Virtru-protected content even without having Virtru installed.
4. **Ease of use:** Virtru avoids the need for additional accounts or for complicated time-consuming manual key exchange.
5. **Confidentiality:** Content and encryption keys are stored separately, so that only authorised parties can access unencrypted content. Virtru can never access unencrypted content or decrypt user content, only recipients authorised by the content creator can access and decrypt protected content.
6. **Open Standards based:** The Virtru Platform uses the Trusted Data Format (TDF) - an open standard XML based file format.

For more information please contact:
t: +44 (0)203 479 5505
w: www.londoncolonial.com
e: compliance@londoncolonial.com