

Accessing Encrypted Emails Guide for Non-NHSmial users

May 2017
Version 3

Contents

Introduction	3
1.1. Purpose of Document	3
Receiving an encrypted email	3
Receiving an encrypted email on an iOS mobile device	5
Replying to and forwarding encrypted emails	6
Register to use encrypted email	7
1.2. Start of registration	7
1.3. Activating your account/Completing the registration	9
Keeping encrypted emails secure	11
Help and further guidance	12
Frequently asked questions	12

Introduction

1.1.Purpose of Document

Target Audience: Recipients of encrypted emails sent from an NHSmial account

NHSmial is a national secure collaboration service for health and social care, designed to enable the secure exchange of information by email and other methods. NHSmial uses the Trend Encryption Micro service to support NHSmial users sending secure, encrypted emails to any email service free global hosted email services such as Gmail/Hotmail and other privately-run email services.

This document provides guidance for recipients of encrypted emails which have been sent from an NHSmial account. It explains how to register for the service, open and read encrypted emails and send an encrypted reply.

It also provides important guidance about information governance and ensuring sensitive information that has been received remains secure.

Please note it is not possible for anyone other than an NHSmial user to initiate an encrypted email exchange using the NHSmial encryption feature. If you are a non-NHSmial user and wish to exchange information securely with a member of health or social care staff who uses NHSmial, please direct them to the document: [Encryption Guide for NHSmial](#).

Note: While encryption guidelines for NHSmial users in Scotland may differ, encryption is recommended as best practice for anyone exchanging sensitive or patient data

Receiving an encrypted email

An encrypted email sent from an NHSmial address (ending @nhs.net) will contain a link to access the encrypted message. The message reads:

PRIVATE AND CONFIDENTIAL

You have received an email message secured by Private Post. Please open the file called Encrypted_Message.htm to read the message.

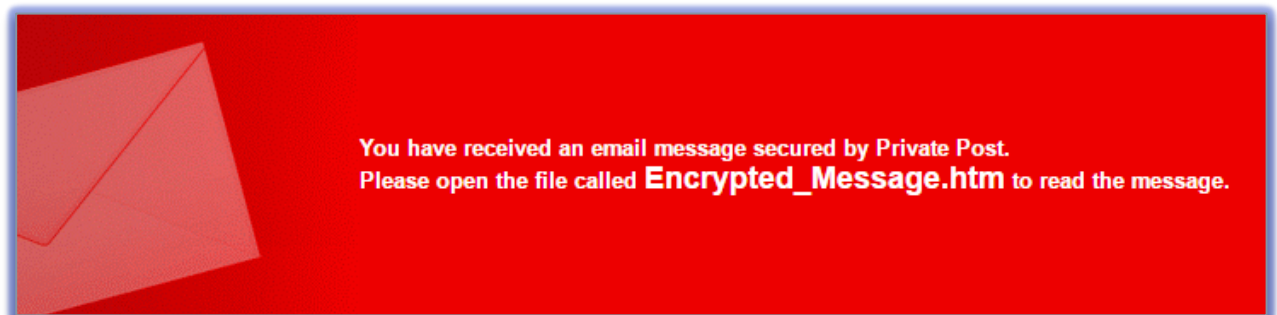


Fig 1. An encrypted NHSmial message in Gmail

1. Open the file **Encrypted_Message.htm**. Your browser should allow you to either view the file directly, or to download and then open the file

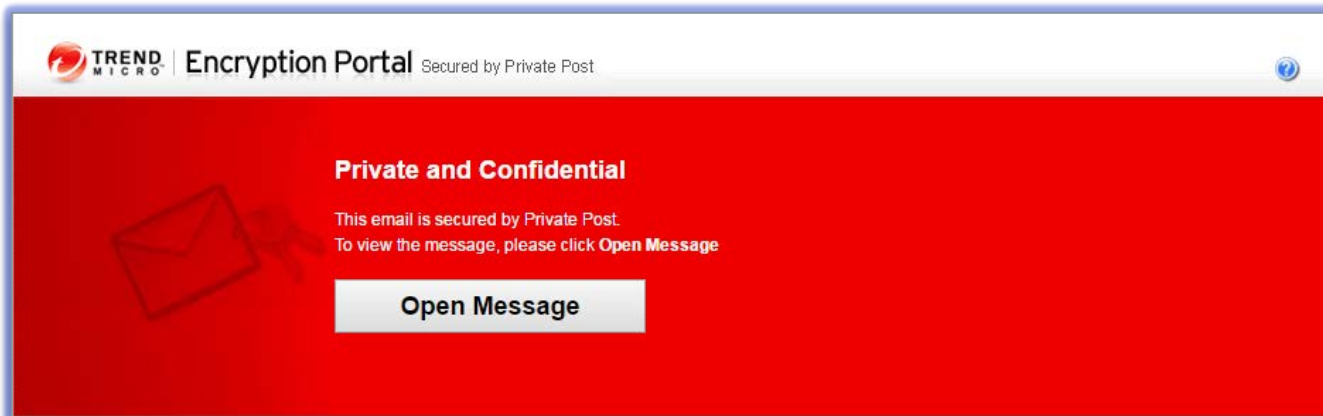


Fig 2. The Encrypted_Message.htm file

2. Click **Open Message** and the account verification screen will appear
 - **Not registered?** If you have not previously received an encrypted NHSmial email, you will be redirected to an external website which will guide you through the registration process to create an account with the NHSmial encryption provider. This should only take a few minutes. See [section four](#) of this document.
 - If you have previously registered with the NHSmial encryption provider, the system may display the **Account Verification screen** (Fig 3).
3. If the account verification screen does not display your correct email address, click **Change**
4. Enter your **Password**
 - Or click **Forgot your password or answers?** if you have forgotten your password.
5. Select a time from the **Keep me signed in** list. For the duration of the time selected, you will remain logged in to the Trend Encryption Micro service. At the end of the time selected, you will be automatically signed out
6. Click **Continue**

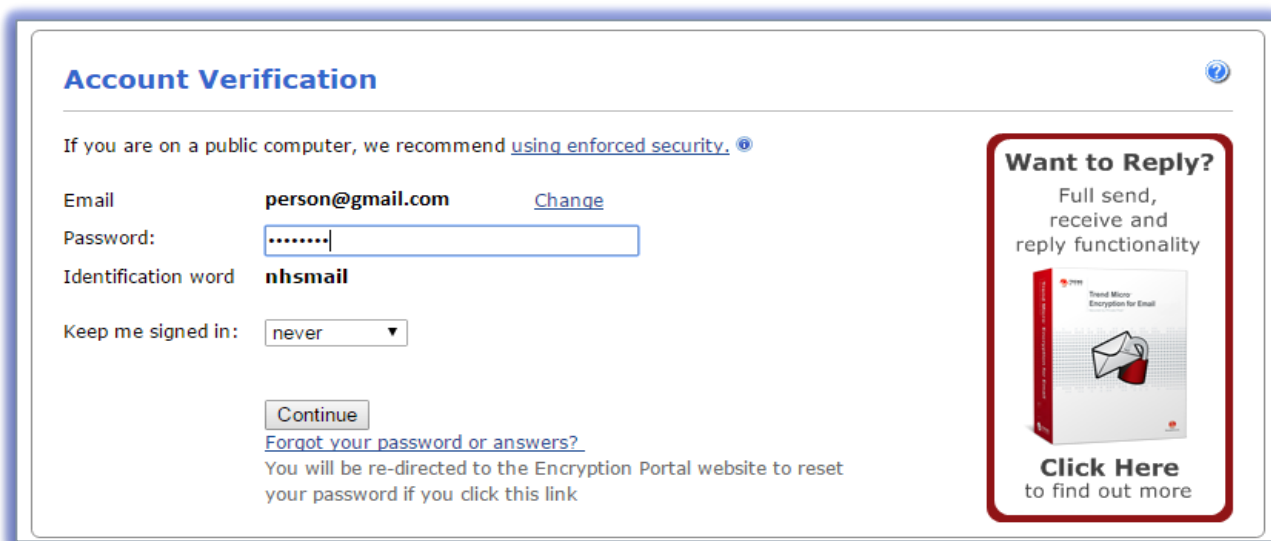


Fig 3. Account Verification

The system will display the encrypted message sent to you from NHSmial.

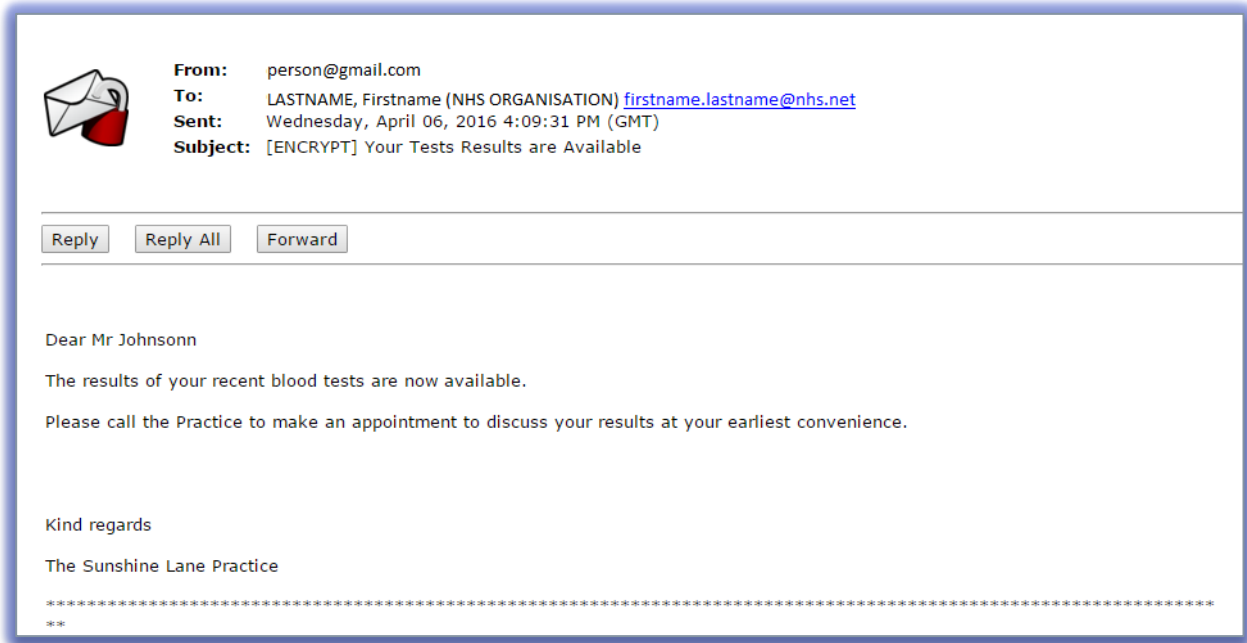


Fig 4. A test encrypted email

You will be able to:

- Read the From, To, Sent and Subject information
- Read the email message
- Reply to the sender
- Reply to all recipients
- Forward the email
- Download attachments

Receiving an encrypted email on an iOS mobile device

There is a known issue with iOS mobile devices (such as iPhones and iPads) being unable to receive encrypted emails. A workaround has been made available for users of these devices and can be found on the Trend Micro website:

<https://success.trendmicro.com/solution/1101512>

The steps to take if you are an iOS mobile device user receiving encrypted emails are:

1. Forward the encryption email that you receive to m@zd.trendmicro.com
2. You will receive a response email with a link in it – you should click on the link which will take you to the Trend Micro website.
3. You will need to login with your email encryption credentials in order to read the content.

The link received is only valid for ten minutes. If you do not login and access the content within this time, you will need to send the email again to m@zd.trendmicro.com.

Once you have logged in, you will be able to reply and forward encrypted emails as necessary.

Replying to and forwarding encrypted emails

You can reply to or forward encrypted emails. Your emails will be automatically encrypted. You can include attachments if required.

To reply to or forward encrypted emails:

1. Open the encrypted NHSmial email
2. Enter your password if the system prompts you
3. Click **Reply** or **Reply All** or **Forward** (as required)
4. Enter the recipients in the **TO:** **CC:** and **BCC:** fields
5. Edit the **Subject** field (as required)
6. Add attachments (as required)
7. Enter a message
8. Click **Send (Any recipient that hasn't already registered to receive encrypted emails will need to go through the process outlined in section 2 before accessing the content)**

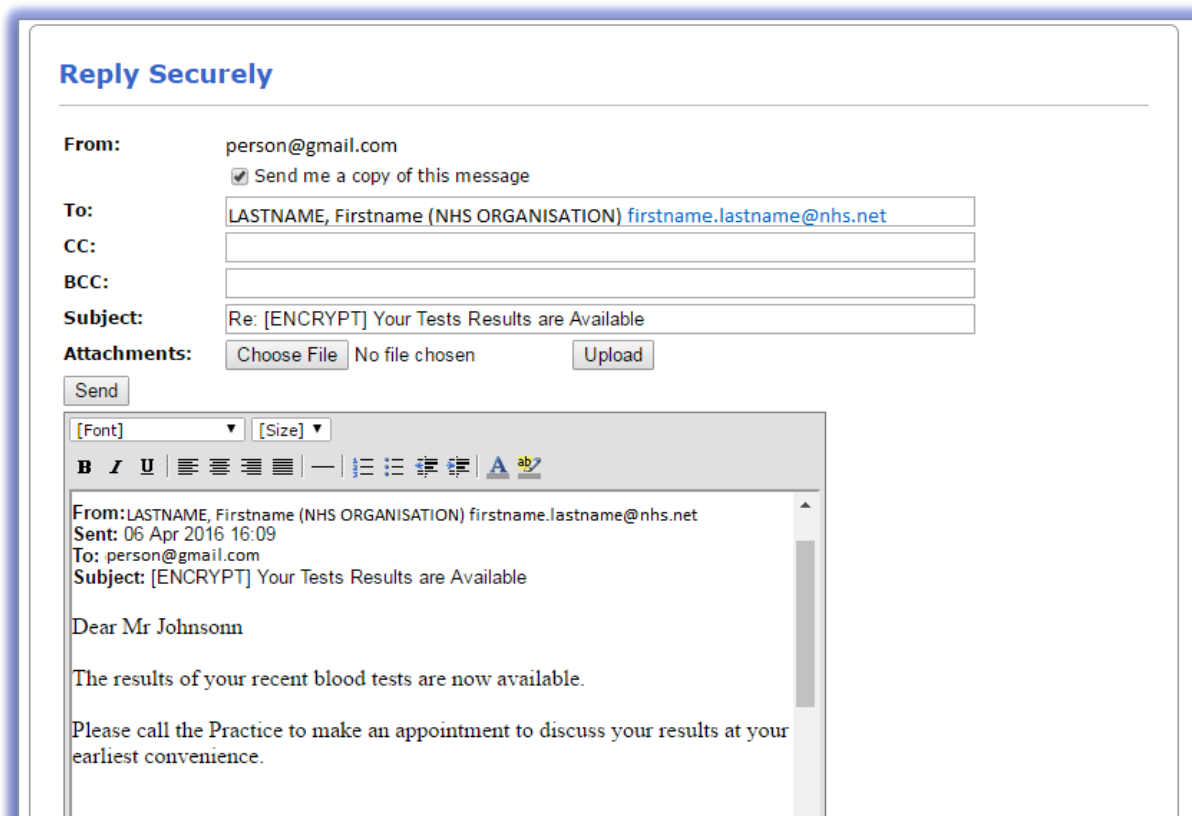


Fig 5. A decrypted email

Register to use encrypted email

If you have not previously received an encrypted email from the Trend Encryption Micro service you will be redirected to the Trend Micro Private Post website. There you will be guided through the registration process to create an account with the NHSmal encryption provider.

Note: Registered recipients don't need to re-register to read subsequent encrypted email messages sent from any NHSmal user.

1.2.Start of registration

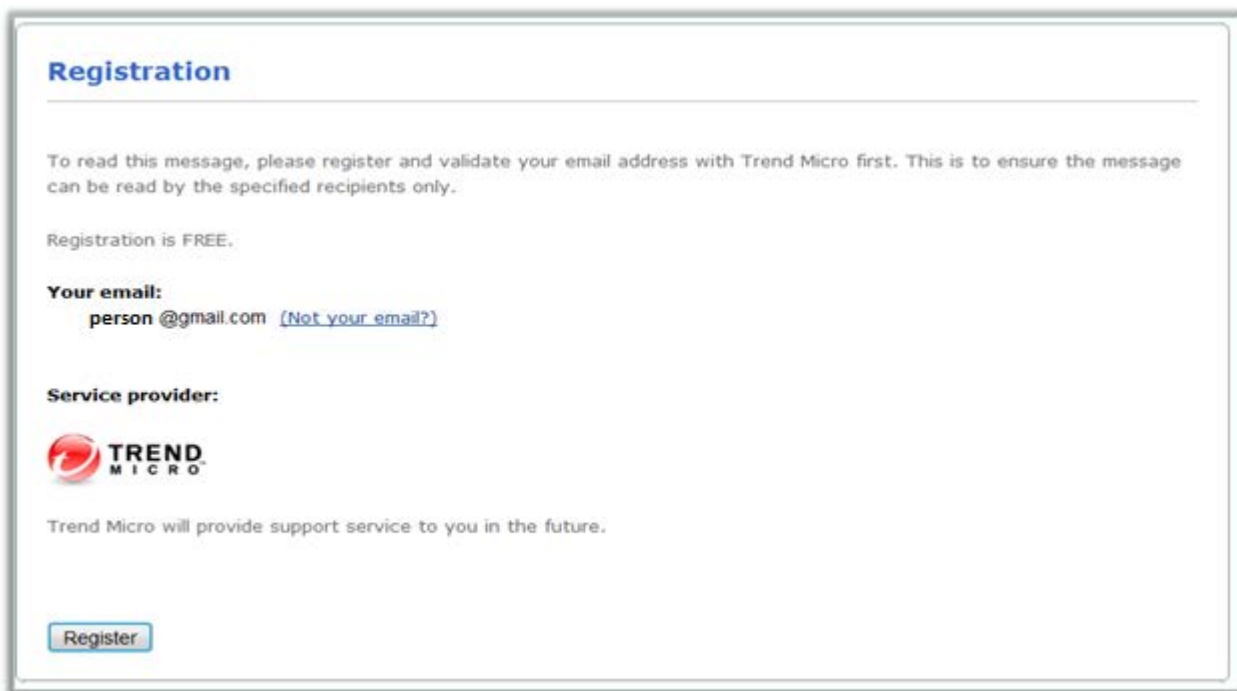


Fig 6. Start of Registration

1. If your email address is not correctly displayed, click the **(Not your email?)** link
2. Click **Register**
 - The **Register Encryption Account** screen will be displayed.

TREND MICRO

Register Encryption Account

Please complete the following information to register your email address.

person@gmail.com will be your identity for encryption. [Change](#)

Select a Password
Your password must be at least 7 characters long. *

Password: [password field]
Confirm password: [password field]
Password strength: Strong

Select Security Question
Select the security question to help us confirm your identity. The answer should be memorable, unique, and contain at least three characters.

Question: [What was your first car?]
Answer: [answer field]

Set your Identification Word
Your identification word will appear on authentication screens, such as the Account Verification and Reset Password screens, to confirm the validity of the screens. Upon seeing your identification word, you can be assured that it is safe to type your information.

Identification word: [word field]
(Minimum 2 characters)

Help us prevent spam and fake registration by typing the code you see in following image.

Type the code: [Q8JJ4]
[Q8JJ4] Change the code
Read the code to me

I have read and agree to the [Licence and Terms](#)

[français](#) [italiano](#) [Deutsch](#) [español](#) [Português](#)

Copyright © 2003-2012 Trend Micro (Encryption) Ltd. All rights reserved.

Fig 7. Register Encryption Account

3. Type and confirm your password – you will need to use this password to open encrypted emails sent to you
4. Select a security question and type the answer
5. Type an Identification word (this will appear on the authentication screens)
6. Type in the code displayed in the “CAPTCHA” image (the obscured code at the bottom of the screen designed to prevent spam and fake registrations)
7. Tick the box to confirm agreement to the Licence and Terms
8. Once you have completed all the fields, click **Continue**
 - The **Check your email to activate your account** screen will be displayed.

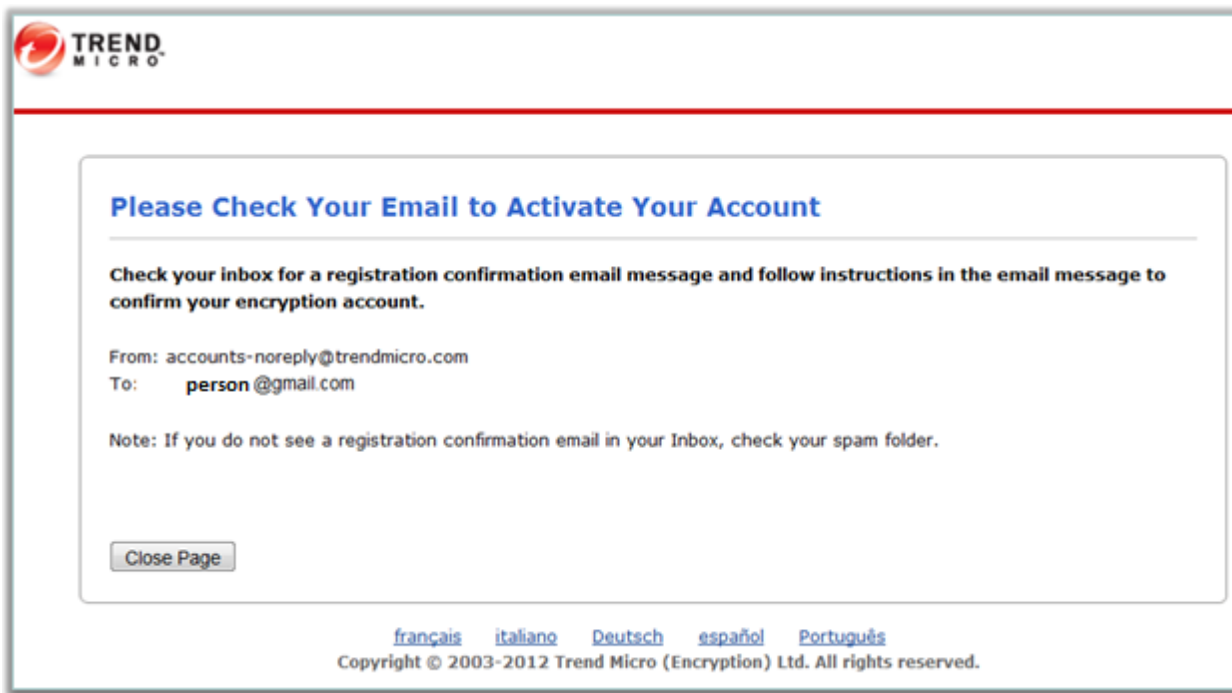


Fig 8. Check your email to activate your account

- A message prompts you to check your inbox for a registration confirmation email message. Follow the instructions in the email message to confirm your encryption account (see next section for more details).

9. Click **Close Page**.

1.3. Activating your account/Completing the registration

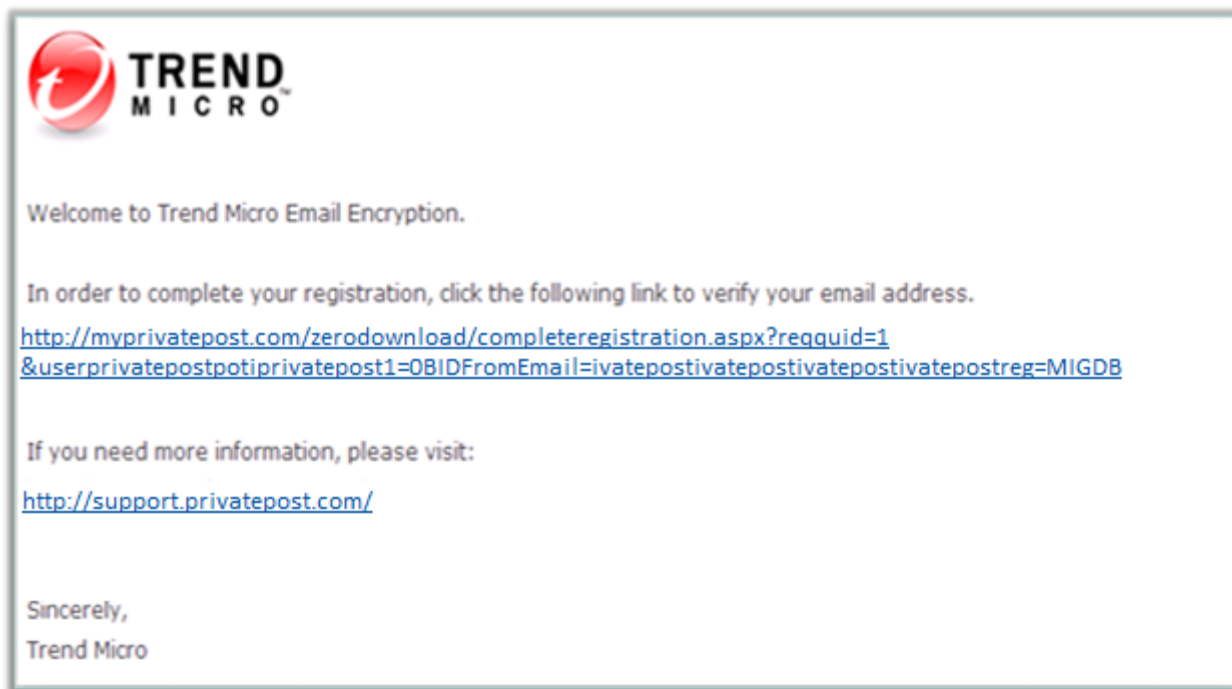


Fig 9. Registration confirmation email message

1. Open the Registration confirmation email message in your Inbox. (If you do not see a registration confirmation email in your Inbox, check your spam folder.)

2. Click the link in the Registration confirmation email message.
 - The **Authentication Successful** message will be displayed.

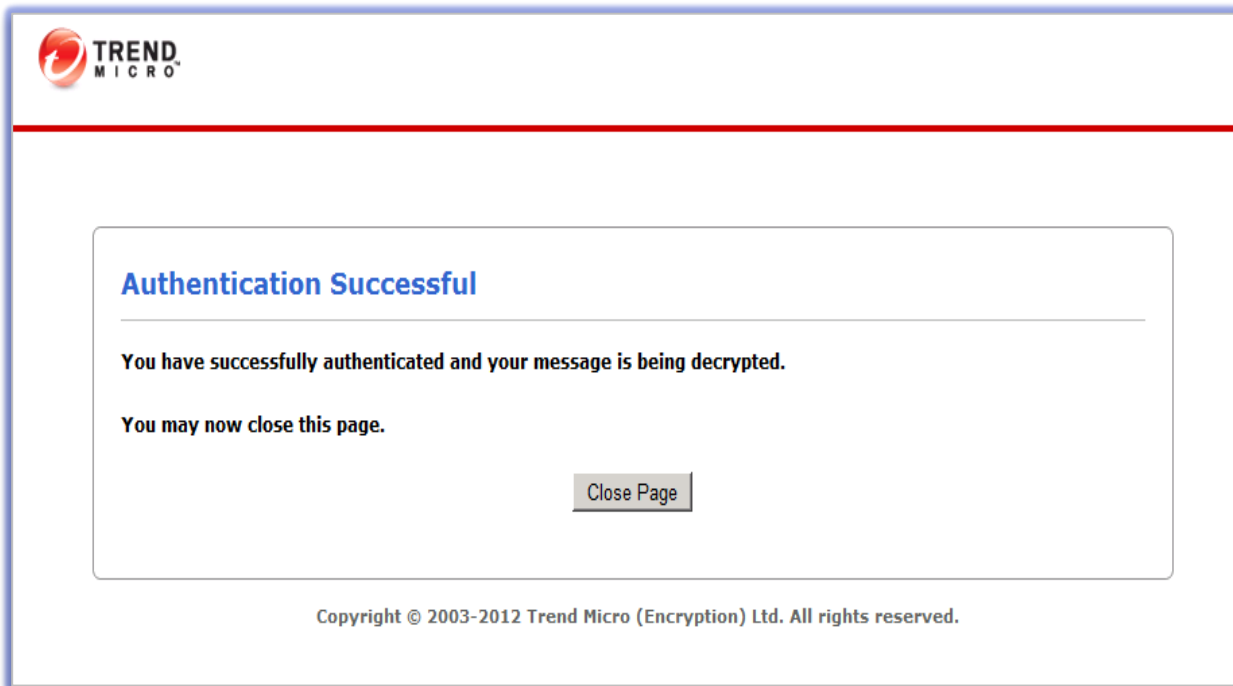


Fig 10. Authentication Successful message

3. Click **Close Page**

This will complete your registration. Once you have successfully registered, you will be able to open, read and download any attachments in encrypted NHSmal emails.

After registration, you can receive encrypted email from any NHSmal user and do not need to register again if another NHSmal user sends you an encrypted email.

To read and reply to another encrypted message you just need to verify your identity using the credentials you registered with when you first signed up to the service. If you forget your password, the system includes a self-service password reset feature.

If another organisation sends you an encrypted email using the same Trend Micro powered email encryption, your Trend Micro account credentials can be used to decrypt these messages too.

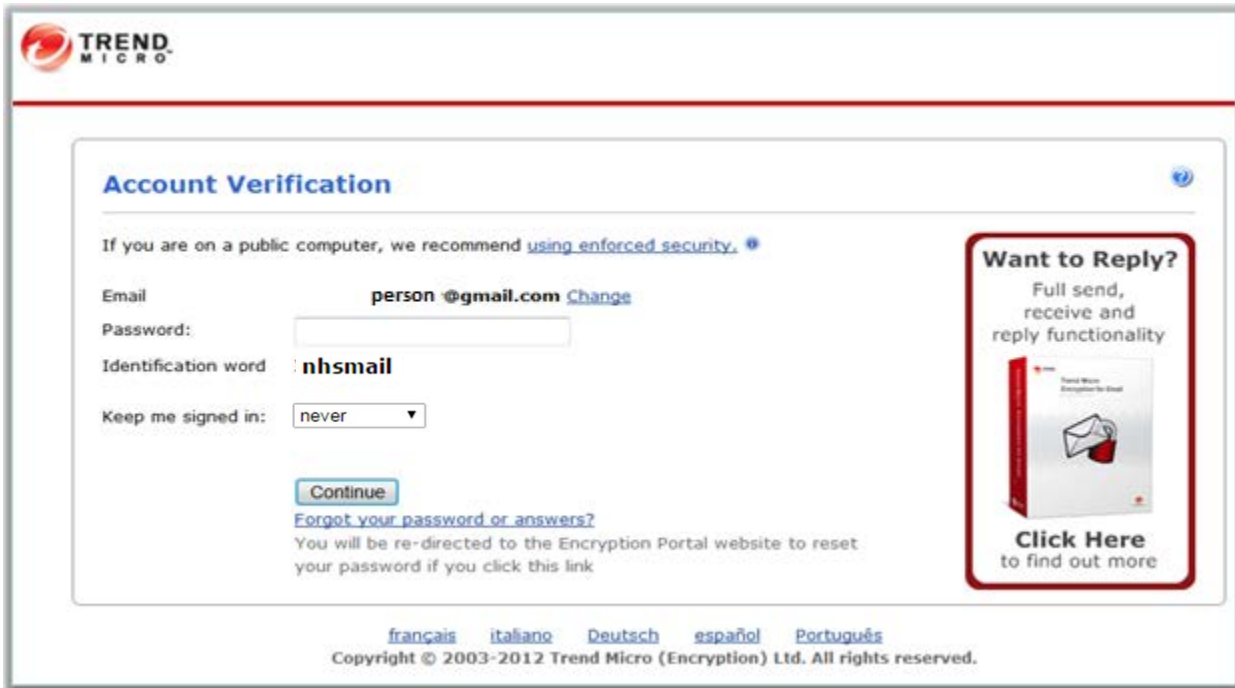


Fig 11. Authentication screen once an account has been created

Note: You do not need to click on the **Want to Reply?** link to use the service. If you click on **Want to Reply** (shown in screenshot above), you'll be given the opportunity to install a Microsoft Outlook 'add-on' that will provide you with the means to send encrypted replies to emails that you receive. You should be aware though that if you install the add-on to a shared computer, someone else could see confidential messages you have received as these will appear in your normal mailbox. Clicking on **Want to Reply** will give full guidance on how to download and install the add-on.

Keeping encrypted emails secure

Before replying to an encrypted email, ensure that the recipient is expecting it and is ready to handle the contents appropriately as part of an agreed clinical or business partner sensitive data workflow, particularly if it contains sensitive or patient identifiable information. If you wish to keep any received emails we recommend you download them and store them safely as required.

Although all attachments sent or received through the NHSmial encryption service will be virus checked we do recommend your organisation runs its own anti-virus software.

Note for third-party/commissioned provider organisations: it is your responsibility, on behalf of your employing organisation, to safeguard any data received in line with the data protection and information governance requirements agreed between your organisation and the sending organisation. If required, you should retain unencrypted copies of any encrypted email received in your local information repositories as per your local information governance policies and processes.

If you are a patient and are receiving information from health or social care staff using the NHSmal service, you should have given consent to the organisation to exchange information with you before they send it. Once received, it is your responsibility to look after any sensitive information sent to you.

You should consider whether the computer on which you access the information is shared with other people – if so they may be able to view any information you receive. There are various excellent sources of guidance on how to keep information secure such as www.getsafeonline.org.

Help and further guidance

For help please visit the Trend Micro support site at:
<http://www.privatepost.com/support/faqs.aspx>

Or call the national NHSmal helpdesk on 0333 200 1133 or email helpdesk@nhs.net
Recipients of NHSmal encrypted emails that require help with registration should refer to the help provided on the registration website.

Frequently asked questions

If I want to forward an encrypted email I've received to someone else, will the email remain encrypted?

Yes. Any recipient added will receive the message securely (encrypted). They will then have to register or log-in to an existing Trend Micro account, as detailed [above](#).

What is the maximum number of email addresses that can be included on a reply to an encrypted email or when the email is forwarded?

You can reply or forward the encrypted email to a maximum of 200 recipients. All recipients will then have to register or log-in to an existing Trend Micro account, as detailed [above](#).

Is message tracking (e.g. delivery or read receipts) available on encrypted emails?

No. Email delivery over the Internet has no guarantees that a message will reach its intended recipient as Internet email can be silently lost.

What is the maximum attachment size I can send on encrypted email replies/forwards?

35Mb.

What types of attachments can be included on encrypted email replies/forwards?

Certain file types that can contain potentially harmful content are blocked by the NHSmal service and cannot be sent or received. The list of blocked attachments can be found in the