CryptoLocker warning

November 20, 2013 in Day to day activities, Incidents, Software, Staff, Students by itsnews | No comments

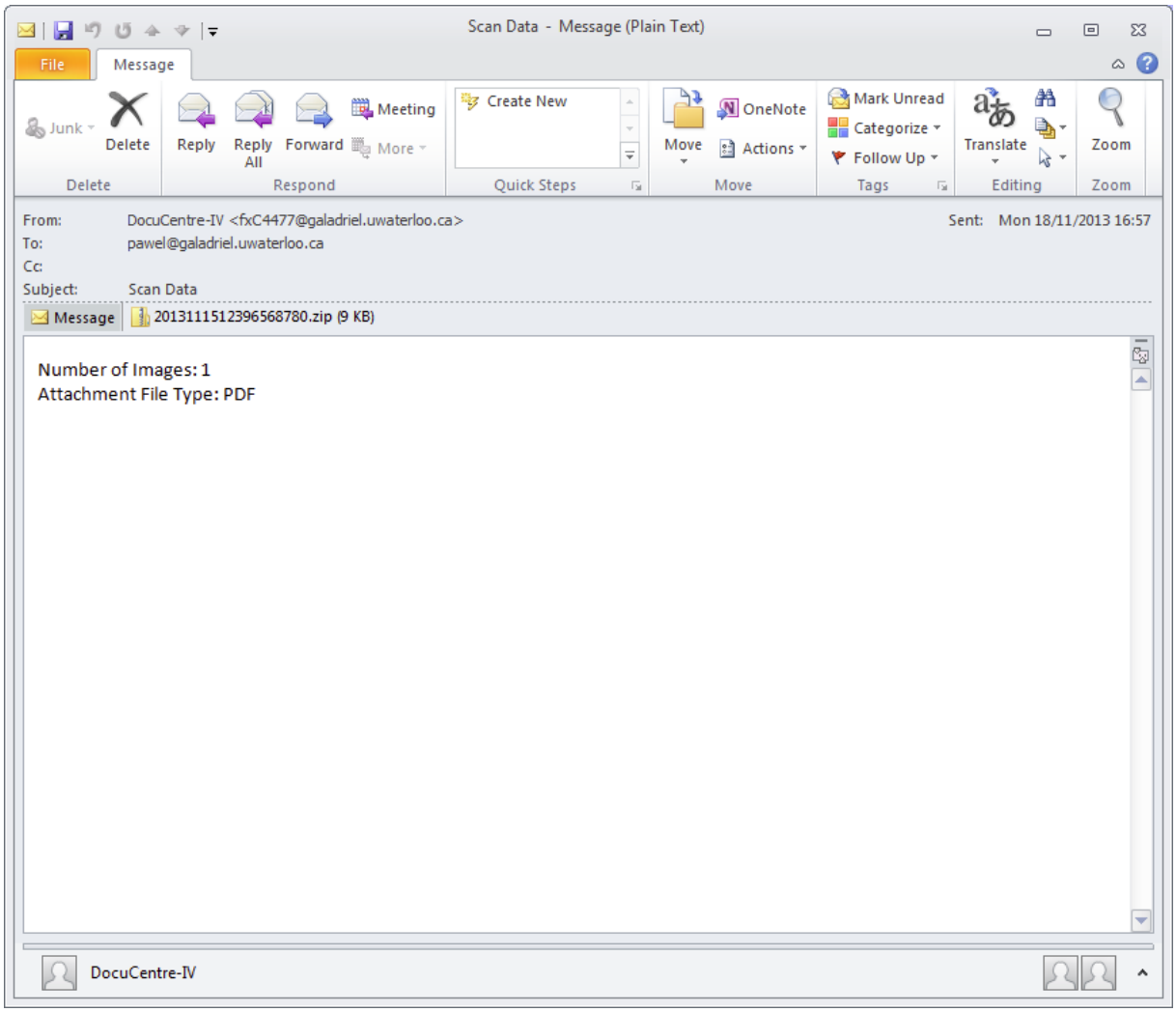
We are advising that you beware fake e-mails such as ones pretending to be either from Voicemail, HMRC, image scanners, courier deliveries, company complaints etc, containing small “Zip” attachments.

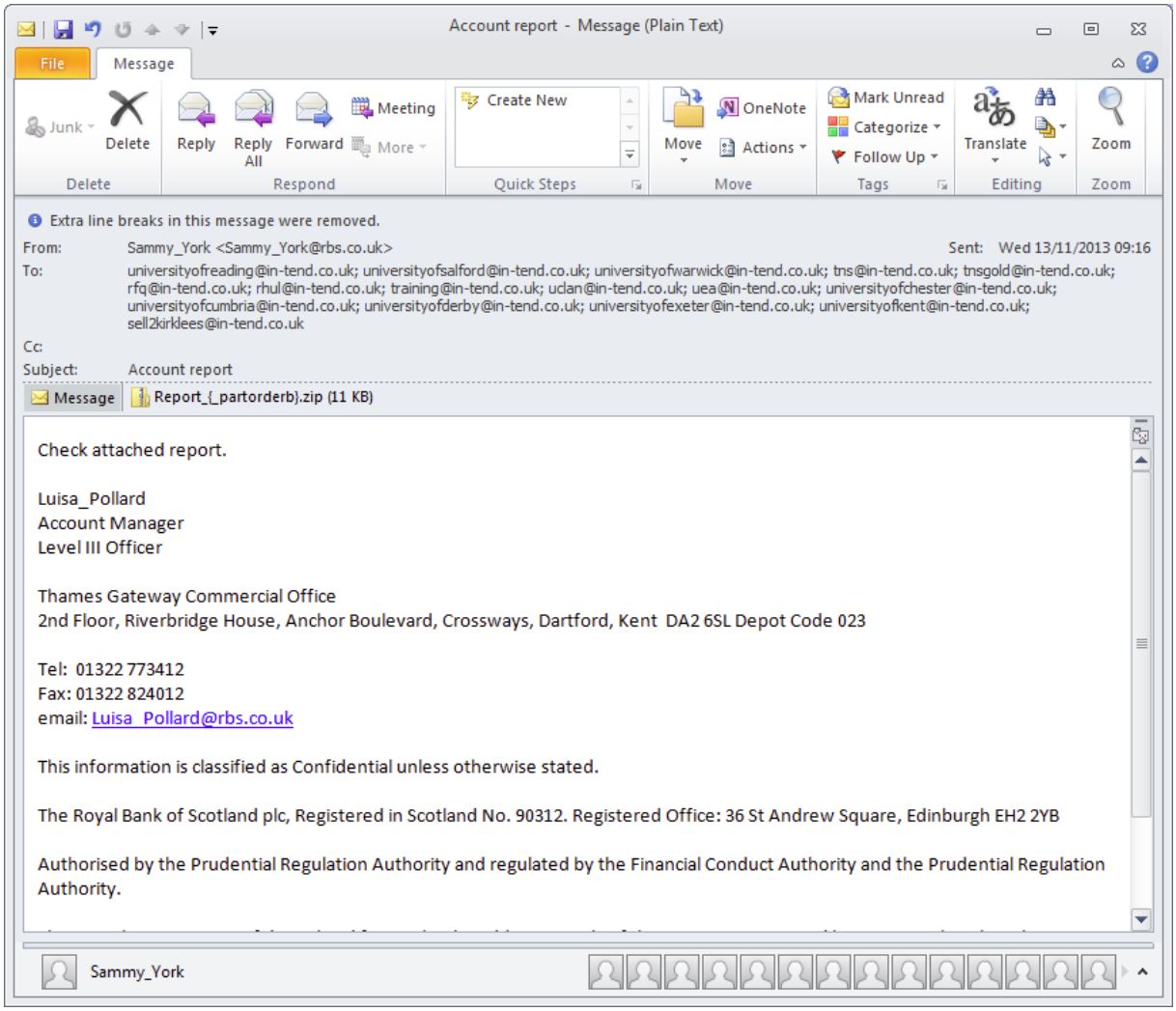
We’ve been seeing quite of few of these sent to University of Reading recipients. Our antivirus scanners have rejected some of them at the email gateways, but others were only marked as spam, and it’s possible some have leaked through.

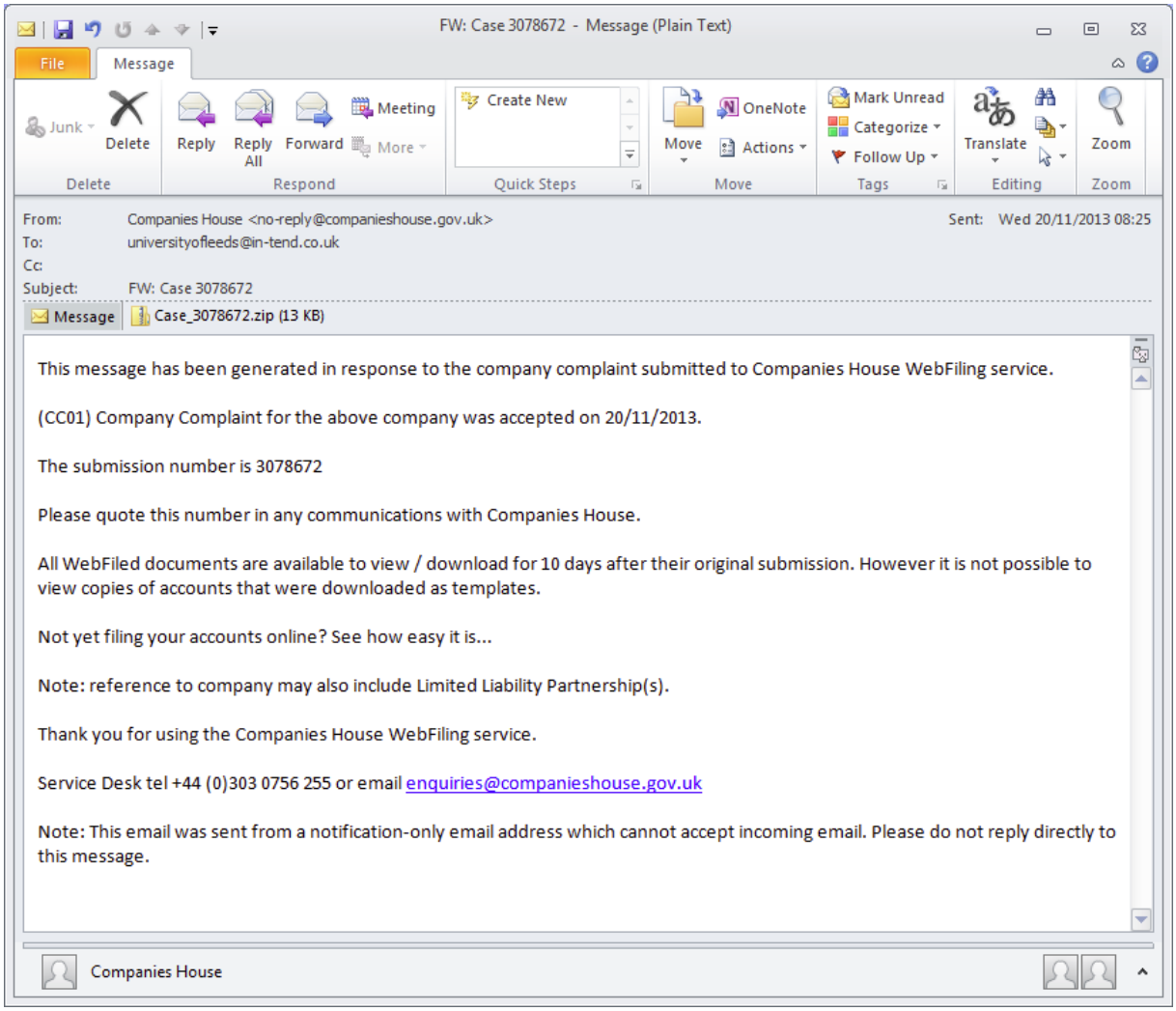
The attachments contain malicious Windows programs which are sometimes cunningly disguised to look like sound, document or image files. These in turn download more malware eventually leading to the installation of the infamous CryptoLocker ransomware. This then encrypts all your files and demands a large ransom to recover them.

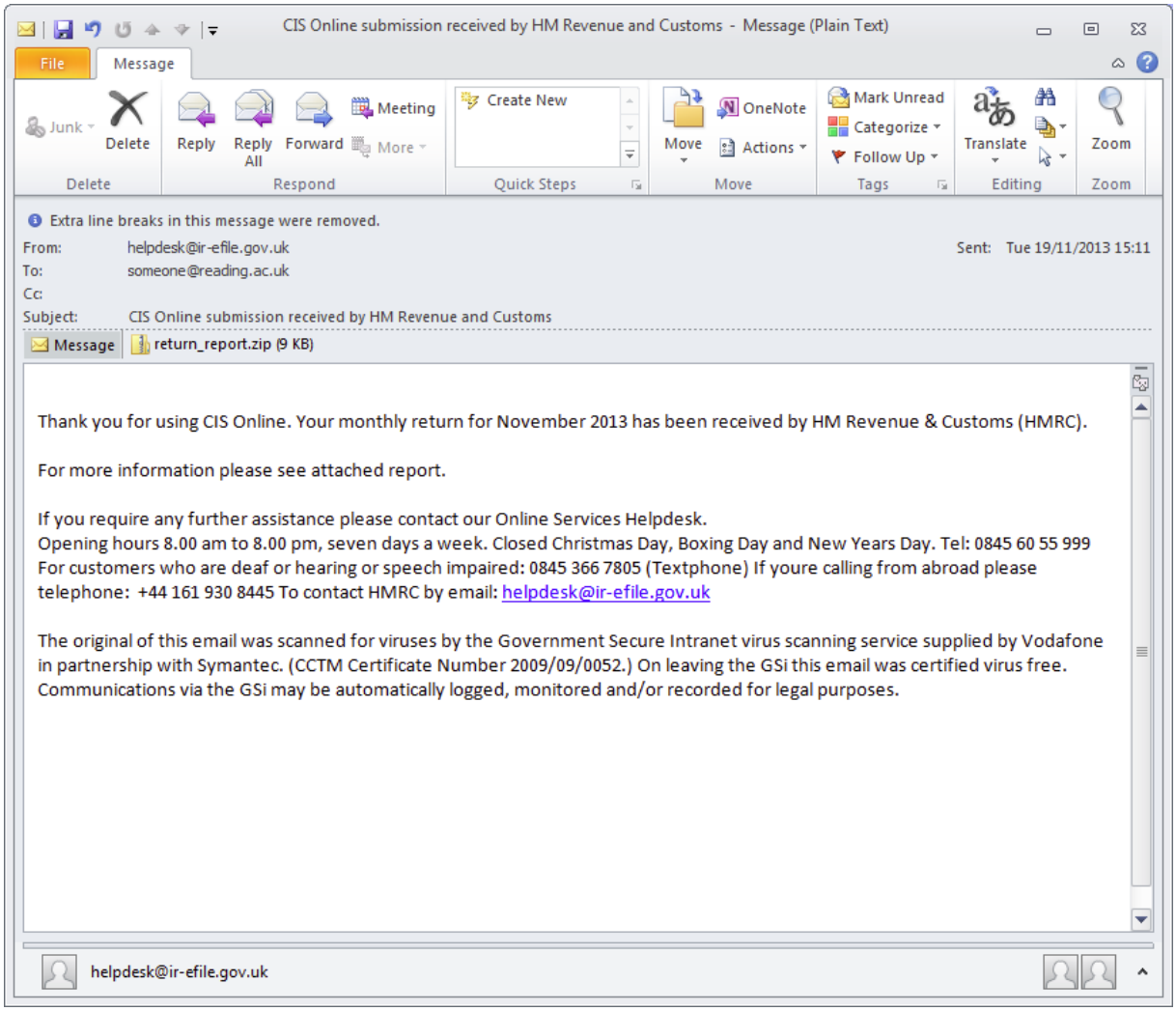
See http://nakedsecurity.sophos.com/2013/11/16/cryptolocker-urge…for more details

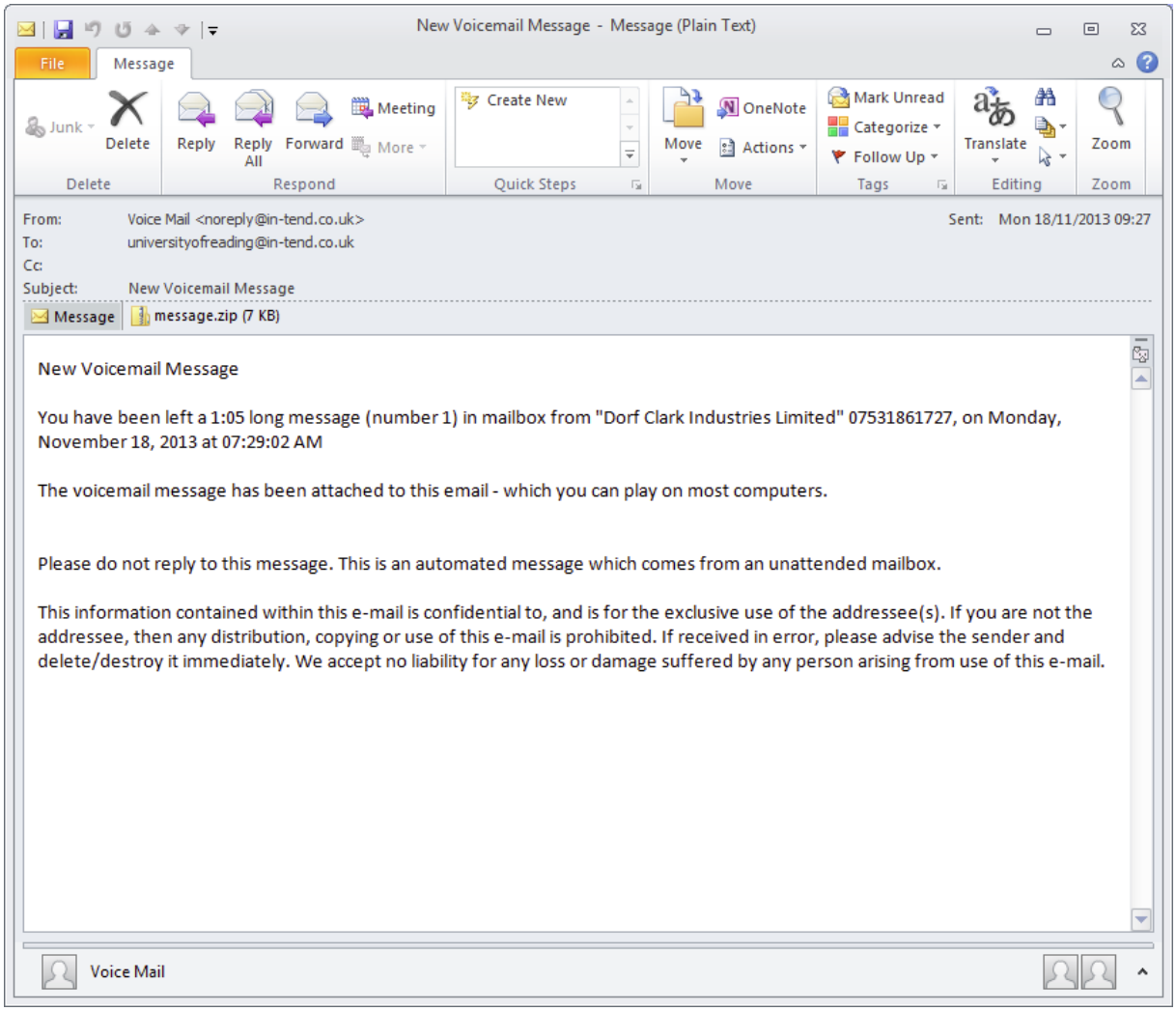
For examples of what the emails may look like, see below:




Account report - Message (Plain Text)
File
Message
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Create New
Move
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
Extra line breaks in this message were removed.
From: Sammy_York <Sammy_York@rbs.co.uk>
Sent: Wed 13/11/2013 09:16
To: universityofreading@in-tend.co.uk; universityofsalford@in-tend.co.uk; universityofwarwick@in-tend.co.uk; tns@in-tend.co.uk; tnsgold@in-tend.co.uk; rfq@in-tend.co.uk; rhul@in-tend.co.uk; training@in-tend.co.uk; uclan@in-tend.co.uk; uea@in-tend.co.uk; universityofchester@in-tend.co.uk; universityofcumbria@in-tend.co.uk; universityofderby@in-tend.co.uk; universityofexeter@in-tend.co.uk; universityofkent@in-tend.co.uk; sell2kirklees@in-tend.co.uk
Cc:
Subject: Account report
Message
Report_{_partorderb}.zip (11 KB)
Check attached report.
Luisa_Pollard
Account Manager
Level III Officer
Thames Gateway Commercial Office
2nd Floor, Riverbridge House, Anchor Boulevard, Crossways, Dartford, Kent DA2 6SL Depot Code 023
Tel: 01322 773412
Fax: 01322 824012
email: Luisa_Pollard@rbs.co.uk
This information is classified as Confidential unless otherwise stated.
The Royal Bank of Scotland plc, Registered in Scotland No. 90312. Registered Office: 36 St Andrew Square, Edinburgh EH2 2YB
Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority.
Sammy_York


FW: Case 3078672 - Message (Plain Text)
File
Message
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Delete
Respond
Create New
Quick Steps
Move
OneNote
Actions
Move
Mark Unread
Categorize
Follow Up
Tags
Translate
Editing
Zoom
Zoom
From: Companies House <no-reply@companieshouse.gov.uk>
Sent: Wed 20/11/2013 08:25
To: universityofleeds@in-tend.co.uk
Cc:
Subject: FW: Case 3078672
Message
Case_3078672.zip (13 KB)
This message has been generated in response to the company complaint submitted to Companies House WebFiling service.
(CC01) Company Complaint for the above company was accepted on 20/11/2013.
The submission number is 3078672
Please quote this number in any communications with Companies House.
All WebFiled documents are available to view / download for 10 days after their original submission. However it is not possible to view copies of accounts that were downloaded as templates.
Not yet filing your accounts online? See how easy it is...
Note: reference to company may also include Limited Liability Partnership(s).
Thank you for using the Companies House WebFiling service.
Service Desk tel +44 (0)303 0756 255 or email enquiries@companieshouse.gov.uk
Note: This email was sent from a notification-only email address which cannot accept incoming email. Please do not reply directly to this message.
Companies House


CIS Online submission received by HM Revenue and Customs - Message (Plain Text)
File
Message
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Create New
Move
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
Extra line breaks in this message were removed.
From: helpdesk@ir-efile.gov.uk
Sent: Tue 19/11/2013 15:11
To: someone@reading.ac.uk
Cc:
Subject: CIS Online submission received by HM Revenue and Customs
Message
return_report.zip (9 KB)
Thank you for using CIS Online. Your monthly return for November 2013 has been received by HM Revenue & Customs (HMRC).
For more information please see attached report.
If you require any further assistance please contact our Online Services Helpdesk.
Opening hours 8.00 am to 8.00 pm, seven days a week. Closed Christmas Day, Boxing Day and New Years Day. Tel: 0845 60 55 999
For customers who are deaf or hearing or speech impaired: 0845 366 7805 (Textphone) If youre calling from abroad please telephone: +44 161 930 8445 To contact HMRC by email: helpdesk@ir-efile.gov.uk
The original of this email was scanned for viruses by the Government Secure Intranet virus scanning service supplied by Vodafone in partnership with Symantec. (CCTM Certificate Number 2009/09/0052.) On leaving the GSi this email was certified virus free. Communications via the GSi may be automatically logged, monitored and/or recorded for legal purposes.
helpdesk@ir-efile.gov.uk


New Voicemail Message - Message (Plain Text)
File
Message
Junk
Delete
Reply
Reply All
Forward
Meeting
More
Create New
Move
OneNote
Actions
Mark Unread
Categorize
Follow Up
Translate
Zoom
Delete
Respond
Quick Steps
Move
Tags
Editing
Zoom
From: Voice Mail <noreply@in-tend.co.uk>
Sent: Mon 18/11/2013 09:27
To: universityofreading@in-tend.co.uk
Cc:
Subject: New Voicemail Message
Message
message.zip (7 KB)
New Voicemail Message
You have been left a 1:05 long message (number 1) in mailbox from "Dorf Clark Industries Limited" 07531861727, on Monday, November 18, 2013 at 07:29:02 AM
The voicemail message has been attached to this email - which you can play on most computers.
Please do not reply to this message. This is an automated message which comes from an unattended mailbox.
This information contained within this e-mail is confidential to, and is for the exclusive use of the addressee(s). If you are not the addressee, then any distribution, copying or use of this e-mail is prohibited. If received in error, please advise the sender and delete/destroy it immediately. We accept no liability for any loss or damage suffered by any person arising from use of this e-mail.
Voice Mail