Soroban Support Guide

Soroban Support

Suspicious emails - look at message headers!

Emails often purport to come from an institution such as a bank and can tempt you to open the email and perhaps follow links.

You should always be cautious and look carefully at any email and this guide tells you how to obtain detailed information about where the source/REALLY is. This information is in the Message Headers and this guide shows you how to access the headers (at least if you use Thunderbird as your email client) nnd gives pointers about what to look for.

If necessary this information can be copied as text into an email for analysis by another party.

Original Author: John Steele
Revised by: John Steele

Version: Draft
Date: 18 Aug 2023

Copyright Notice

Revisions

Version	Date	Changed by	Summary of change
Draft	18/08/2023	John Steele	Initial version

Table of Contents

Table of Figures

Overview

1.1 Suspicious email

It is unfortunately very common to get an email that purports to be from somewhere important such as your bank. There are other emails which are less scary but are also unwanted.

It is not always evident where these emails come from unless you really know how to find out.

This document attempts to give you the information to help you find out whether it is genuine but can also help you collect the information for you to get further help from an expert.

1.2 The challenge!

The main challenge in helping you with this problem is that there are many ways in which you can read your emails.

Each method can, as far as we know, enble YOU to get the information but the method of finding it depends on which method you use to read your email.

1.2.1 Webmail

In general you will either read your email by accessing a web page and read your email via a browser such as:

- Microsoft Edge
- Chrome
- Safari if you use an Apple Mackintosh computer
- Or a whole host of alternative browsers

Each of these browsers can access your web mail and it now depends o which service you use to handle webmail. For example:

- Microsoft Hotmail or Outlook
- Gmail provided by Google
- There are many others!

This type of access is generically referred to as Webmail

1.2.2 Mail Client

You may choose to use an email program on your computer to download email to your computer. Again many such email programs exist. The list includes:

- Microsoft Outlook
  - This is the default Email program is you use Microsoft Office
- Microsoft Mail
  - This is installed on current versions of Windows
- Thunderbird
  - This is a free, open source, email client that is widely used
  - It is available for most platforms
  - It is the email client used by the author of this document

There are many other email clients and each has its own features and benefits. Specific instructions on how to investigate where an email program can be added to this document if the necessary information can be provided to the author.

2 HOW DOES AN EMAIL WORK?

2.1 Email routing data

All emails contain some heading data that tells the recipient where is has come from and to which email it is addressed to.

This information is typically not important to the recipient, contains a lot of detailed information about the email which is normally not relevant to the person receiving the information and your email client does not normally display it.

This heading data however can be maliciously misused to give the impression that the email comes from another source.

Most email client programs provide the means to look at the message headers which is what you need to really check what is happening.

It is usually possible to copy the header information and paste it into an email so it can be sent to another person if you are not able to investigate it yourself.

2.2 Examples using Thunderbird

To illustrate the email you see in your email client using a test message. SeeFigure 1 Typical email below.

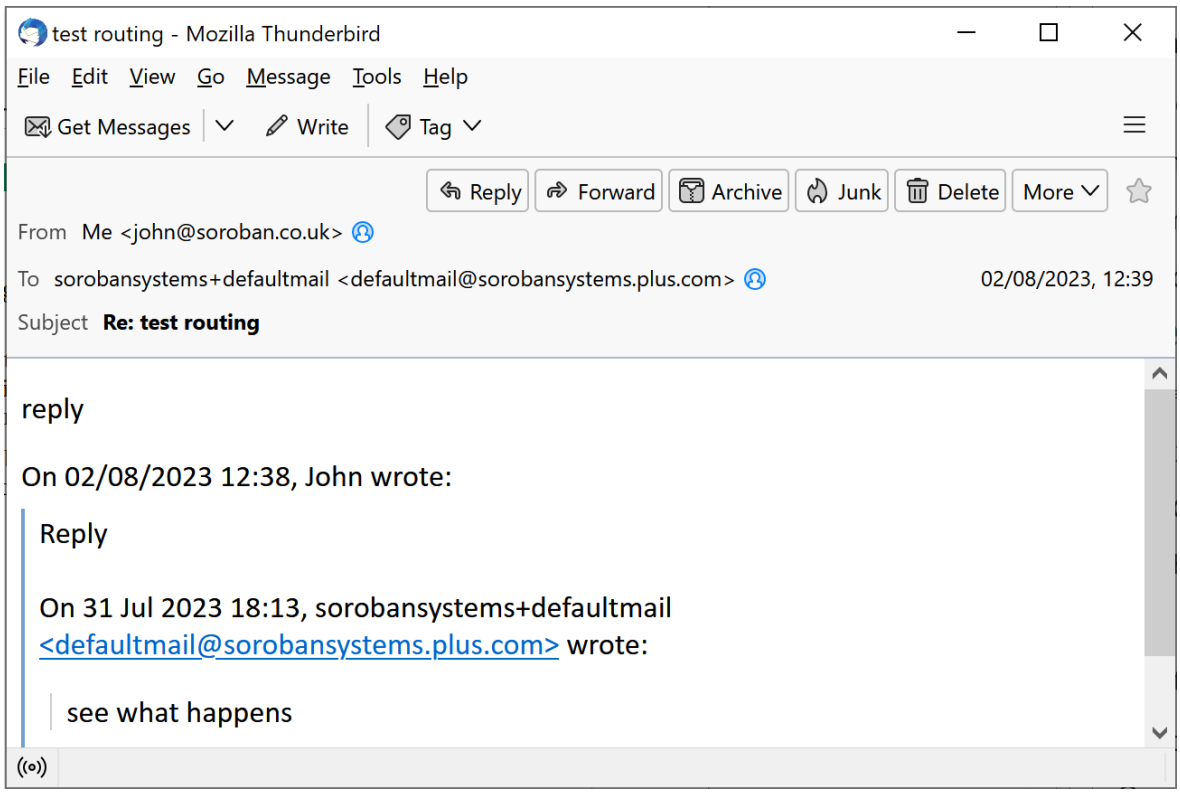

Figure 1: Typical email

This is a screen captured from a Thunderbird email program on a Windows computer. It shows that the email came from john.steele@soroban.co.uk and was sent to defaltmain@sorobansystems.plus.com.

To see more detail in Thunderbird you click on ***View*** and then you will see another options menu see Figure 2: View message source below, Click ***Message Source*** to see the message in all its detail.

Note that the email is NOT one of the suspect phishing emails!

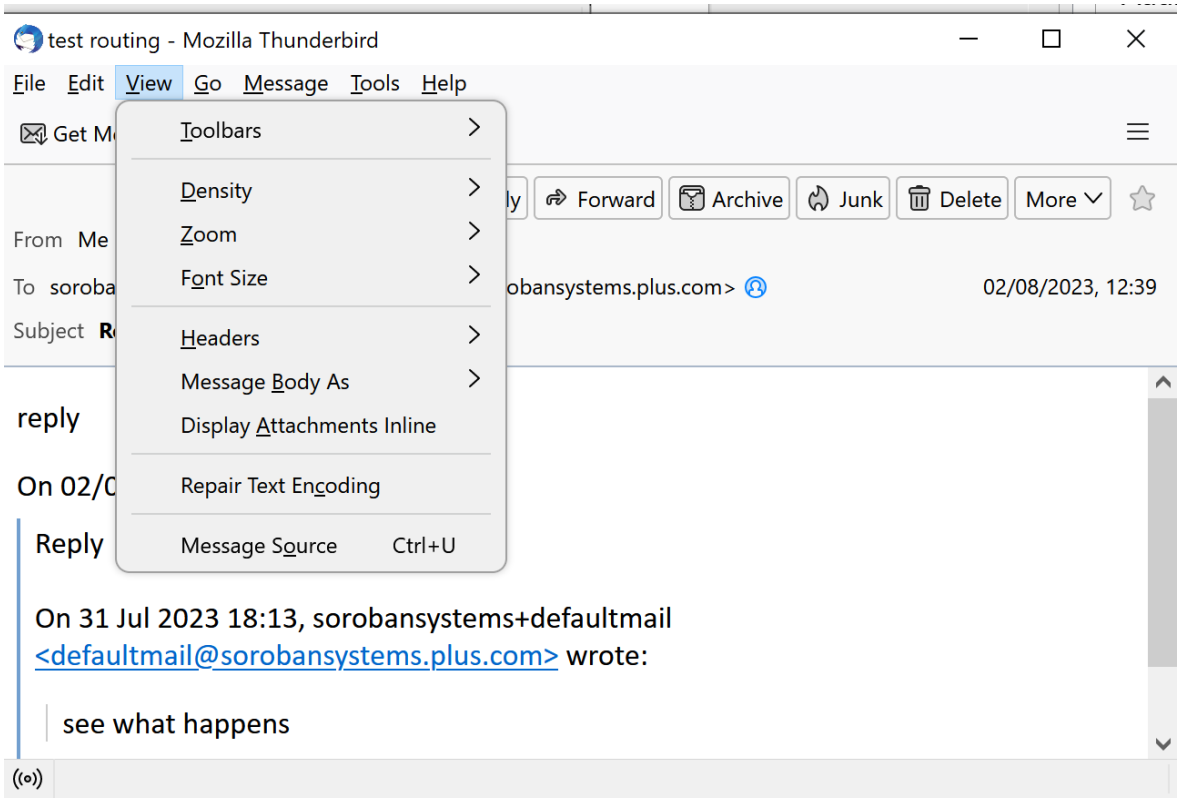

Figure 2: View message source

The next step is to click on ***Message Source***

This will produce a text window as shown below (it has been "pruned" to remove some less important data.). This was from real message that was actually picked up by my SPAM filter unlike some suspicious emails – don't assume that this will also detect them.

The email was addressed to jcs.comodo@soroban.co.uk

This email appears to come from twitter@concord.com.mx and there severl other messages that refer to other apparently related servers.

```
From - Wed Aug  2 09:46:56 2023
X-Account-Key: account16
X-UIDL: UID337-1690376351
---
Return-Path: <twitter@concord.com.mx>
----
X-Original-To: jcs.comodo@soroban.co.uk
Delivered-To: defaultmail@soroban.co.uk
Received: from concord.iservidorweb.net (unknown [191.96.145.18])
        by my_email_serverk (Postfix) with ESMTPS id 206966E958
        for <jcs.comodo@soroban.co.uk>; Wed,  2 Aug 2023 06:47:27 +0000 (UTC)
Authentication-Results: my_email_serverk;
        dmarc=none (p=NONE sp=NONE) smtp.from=concord.com.mx header.from=concord.com.mx;
        dkim=temperror header.d=concord.com.mx;
        spf=none (sender IP is 191.96.145.18) smtp.mailfrom=twitter@concord.com.mx
smtp.helo=concord.iservidorweb.net
Received-SPF: none (my_email_serverk: no valid SPF record)
Received: from bbijril (unknown [181.214.218.59])
        (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
        (No client certificate requested)
        by concord.iservidorweb.net (Postfix) with ESMTPSA id 04B2374BC879;
```



```
        Tue,  1 Aug 2023 19:17:11 +0000 (UTC)
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=concord.com.mx;
        s=default; t=1690917440;
        bh=mVkgS+lyjzzePw8hsRYRj1qcyq0L5eUG3RIwDtxiDA8=;
        h=Reply-To:From:To:Subject:Date;
        b=NGT+ZX1JV0S1SzxI5tpn8JROiITcNAXhHKi0xWSynLhtTxPFFc1LItD2oq5zuqgFA
         ElgKWCAFR9i1NI1KZ7mGYFkdfvFX65uUO5K84gT8LihHBvsJ98prACSClcxddyZAiN
         m6t93xifa5ulMRpQEky1UIhHYAe0OLEPAGbh1cHI=
Message-ID: <0dd88922d6123833152f66cd39efc5ceeb03274f@concord.com.mx>
Reply-To: Wilma Broderick <WilmaVJIUOBroderick663@falasteen.cc>
From: Wilma Broderick <twitter@concord.com.mx>
To: john@atypica.com
Subject: ***********-edited
```

