Safe Move Scheme Login Security Policy

Keeping Your Data Safe Online

Created October 2015. Version 1.0

Contents

Introduction

We want to ensure that you use the Safe Move Scheme (SMS) safely and that your data is kept securely. By following the Safe Move Scheme Login Security Policy you reduce the risk of your data being intercepted by 3rd parties and you increase your safety.

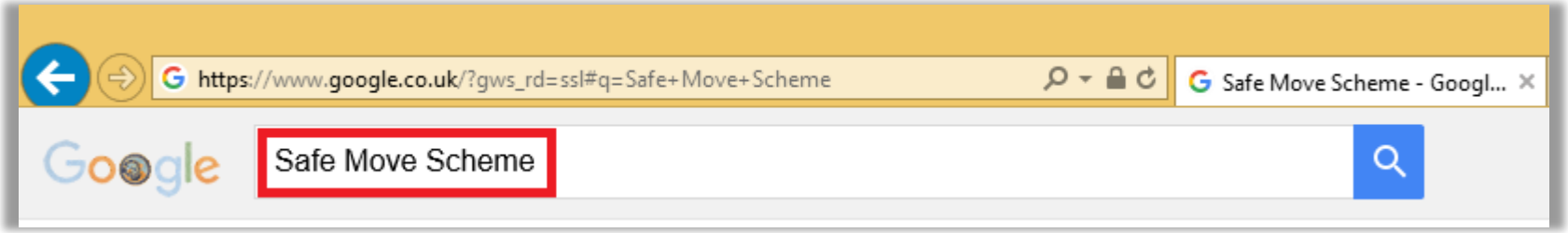
The Safe Move Scheme is a secure website portal and has been built by our data security experts to ensure that the data passed to it is kept securely. We continuously test the security properties of our website and we update cybercrime threat risks on an ongoing basis. Our website has the highest security certification possible, however, it is **essential** that when you log in to the Safe Move Scheme you have not been taken to a bogus website[1] and end up relying on misleading information as a result. This document will help you stay safe.

This document also sets out how we communicate with our users. It is **essential** that users understand how we communicate so they are not tricked by following procedures that are not used by the Safe Move Scheme.

[1] A bogus website will use website addresses which are very similar to the authentic website address (i.e. there may be one or more letters difference). Bogus websites hope the user does not notice these differences and logs in or enters sensitive details. For example: http://www.safemove scheme.co.uk (omitting the 's' from 'https'); or http://www.safemovesscheme.co.uk (adding an extra 's' to 'move')

Use the following instructions from a secure Wi-Fi network - **never** log into the Safe Move Scheme using an unsecured or unknown network (such as a publically available network).

Step 1 - Google 'Safe Move Scheme'



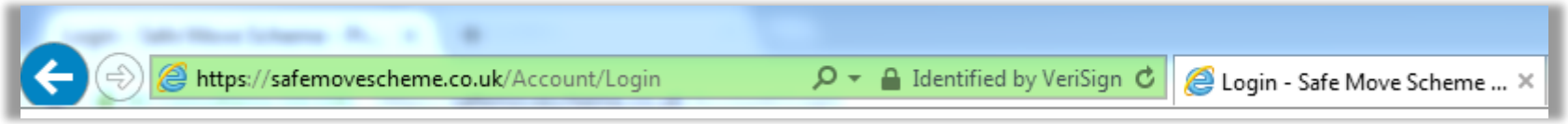
Step 2 – Select the Google result that matches Safe Move Scheme

Step 3 – Click the login icon at the top right side of the screen to go to the SMS secure portal login screen

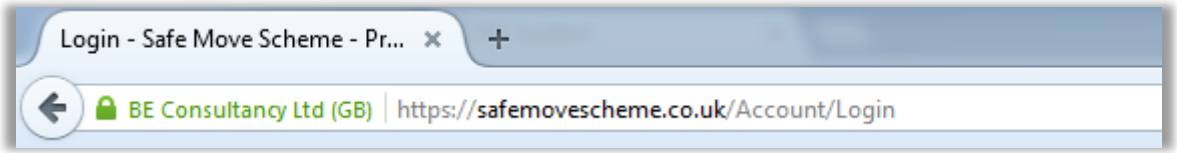
Step 4 - The address bar must match one of the following images below depending on which internet browser you are using:

Chrome (v.46.0.2490.80) -

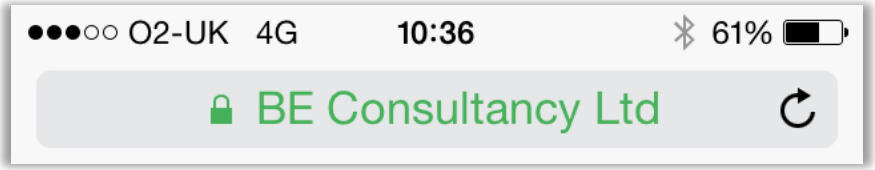
Internet Explorer (v.11) -



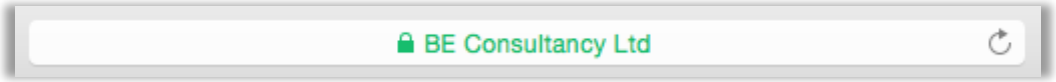
Firefox (v.41.0.1) -



iPhone/iPad iOS (Safari v.9) -



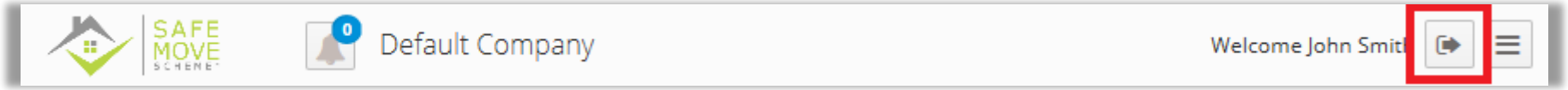
Mac OSX (Safari v.9) -



It is essential that you login to the correct URL (i.e. website address) and to **ALWAYS** check that the URL window contains the green padlock and 'BE Consultancy Ltd' text which matches the appropriate image above.

When you have finished using the Safe Move Scheme secure portal, always remember to **log out** and close the browser window you used to access the portal.

Use the '*Log out*' icon (shown below) to log out of the Safe Move Scheme secure portal – this will take you to the SMS secure portal login screen at the website address shown in Step 4 above.



Email – **emails are not safe** (as it's not possible to prevent emails being intercepted by hackers)

We will **never**

- email you sensitive data
- email you a link to our SMS secure portal login screen
- email you an attachment

You must **never**:

- email us sensitive data
- click on a link claiming to take you to the SMS secure portal screen
- open attachments claiming to be from the SMS
- forward an email you suspect is not from the SMS
- reply to an email you suspect is not from the SMS

We will:

- Send email alerts asking Users to log in to view notifications
    - Users can only view notifications by logging into the SMS secure portal using the secure login procedure described in the Logging In section above
- Respond to general queries via email that do not contain sensitive data

You can:

- Email us general questions
    - please consider that this message has potential to be intercepted by a 3rd party (including hackers) and therefore must not contain any sensitive data that may compromise your security

Phone – We may call Users to discuss their SMS account

We will **never**:

- ask a User for their password or PIN
- ask a User to log in to another website
    - always follow the secure login procedure in the Logging In section above.

We may:

- ask you to login – always follow the process as detailed in the Logging In section above

Text Messages – We may text information to Users in relation to their SMS account

We will **never**:

- ask a User for their password or PIN
- ask a User to log in to another website
    - always follow the secure login procedure in the Logging In section above.
- text you a link to our SMS secure portal login screen

We may:

- ask you to login – always follow the process as detailed in the Logging In section above
- provide some security details for your login

Website Links

We will **never**:

- email a link to the SMS secure portal login screen

You must **never**:

- log in to a website using a link from an email

Compromised Data

If you believe your security has been compromised please change your password as soon as possible by using the SMS secure portal.

If you believe any details regarding you or your transaction have been changed without your consent, please contact the supervisor that is responsible for your account (this could be your conveyancer or SRO).