Phishing email scams and Institute policy on emailing our Members and Fellows

The Institute is aware that its name may be misused to perpetrate fraud, and that fraudulent activities including phishing scams are growing across the shipping sector. As membership subscriptions are now due, we want to ensure that making payments to the Institute is convenient and accessible for members, and that we protect our members as much as possible.

One technique (known as phishing) is to issue emails to our members claiming to originate from the Institute, either our head office or a local branch, and which may also provide links to fictitious financial web sites. You may receive an email that looks like it comes from us asking you to log on and check your account. It looks real, so you might be tempted to click on the link and enter your user ID and password into the website.

Phishing scams are used by criminals to lure victims, by email, text or phone, into handing over valuable information such as credit card and bank account numbers, passwords and log on details, which can be used to commit fraud. We will never send you an email, text or a website link asking you to enter your Internet Banking or card details.

What to look out for

Impersonal greetings and probing questions

A phishing email will not be personally addressed to you but may begin with 'Dear valued member'. The fraudster or fraudulent website may ask for lots of sensitive personal information such as passwords, Internet banking log on details, contact details or credit card numbers.

Urgent warnings

A phishing email may say things like 'we need to verify your membership information' to try and get you to respond without thinking.

Bad spelling and formatting

The wording of the email may have poor grammar and spelling. The fake website may look slightly different with an alternative layout or misspelt words.

Display name

Sometimes the display name of the sender in an email can be misleading. You can confirm the actual email address by double clicking on the display name.

Links in the email

A counterfeit site can be used to collect log on credentials and information intended for the genuine site. In emails, website addresses may appear genuine on first sight, but if you hover your mouse pointer over the link without clicking, it may reveal a different web address.

Genuine emails

We will always:

Quote your membership number.

- Greet you personally using your title and surname.
- Use links in our emails that will only ever to go to www.ics.org.uk or www.shipbrokers.org .
- We will never link directly through third party websites or ask for your personal details.

If you are concerned

If you have received an email communication purporting to be from the Institute and you are concerned over its legitimacy, please contact membership@ics.org.uk with a subject of "Email Abuse" and include details of its contents, providing a copy where possible.

We recommend that you do not click on any web links contained within these emails as they may expose your computer to viruses or spyware and that once you have reported the matter, you delete them. You may also wish to contact the internet service provider from where the email has been delivered to report "Email Abuse" and request that any messages from the relevant account are blocked.

Membership subscriptions and other payments to the Institute

The Institute has invested heavily in our online membership database. This database is accessed only by user name and password. Our office team and branches do not have access to your password and will never ask you for your password. If you cannot remember your password then please use the '**FORGOT PASSWORD**' function to receive a new password.

Payments through this system are made securely via Sagepay, and the Institute database keeps no records of banking or credit card information. We recommend to members that payments via this database are the fastest and more secure way to make payments.

Payment through other methods

If you don't wish to pay online, you can pay via bank transfer or credit card via fax.

If payment is by bank transfer, please ensure you use only the bank details given to you directly by the Institute or, if required, your local branch. We are aware of attempts to issue fraudulent invoices with modified bank details across the shipping sector, especially affecting those members working in port agency. Advice from ITIC - International Transport Intermediaries Club, can be found in the news section of the Institute's website.

If you think an invoice sent to you may be fraudulent, please phone the Institute on **+44 (0) 20 7623 1111** or phone your local branch. Please don't reply directly to the email but instead re-enter the email address from a previous message that was accepted as being authentic. Similarly, please don't call a telephone number in the fraudulent email, but instead call us using the number published on our website: ww.ics.org.uk.

Credit card by fax

If you wish to send your credit card details to us, you must only send these via fax to **+44 (0) 20 7623 8118** and **never via email**.