Circular From NORTH
Date: 21 March 2018

Cyber Fraud - A Continued Threat

North has learned of further cyber fraud attempts from its correspondent in China.

Reported attempts include fraudsters pretending to be correspondents, brokers or claims handlers in P&I clubs. On some occasions the email accounts of correspondents have been hacked, and funds requested in relation to a claim.

In other cases false claims have been fabricated and emails sent to P&I clubs or directly to the Members.

Some emails contain attachments with viruses embedded in them in order to gain access to the receivers email account.

The email addresses being used can appear legitimate, however are often changed by a single character.

If asked to redirect funds by email always double check by calling the intended recipient of funds using a phone number you know to be correct.

Recommendations

1. Please check the email addresses of the senders. Most of the fraud emails are sent from addresses that are different from the real ones, which can usually be easily detected. By doing this, you will be able to screen most of the fraud emails.

   However, please note that even if the email address appears correct, it doesn't mean that the email is one hundred percent safe; that's why the following points are even more important.

2. When payment or remittance is to be made, extra care should be taken. Please make sure that you will telephone the intended receiving party in person to verify the bank account, should account details be found suspicious, especially when the fund is requested to be remitted into a revised bank account.

3. If possible please increase the security level of the email settings including password, logging record monitoring, etc. and update the anti-virus systems timely.

Full circular can be read here.

Source of Information: North of England P&I Club