23 May 2019

Countering external fraud - phishing

Members will be aware of 'phishing', the practice by which a third party fraudster poses as a genuine party to illegitimately intercept funds (meant to be paid to the genuine party) and/or to gain access to sensitive information. In simple terms, the fraudster joins legitimate correspondence by posing as one of the parties. For example, a genuine third party's email address may be XYZ@cargo.com but the fraudster manages to join the exchange by using the email address XYZ@carg0.com. If other parties use 'reply all', the fraudster is then added to all future exchanges and can monitor developments, including when and to where any future payments are to be made.

Fraudulent activity of this nature can take place over a period of weeks or months, with no immediately obvious sign that messages are being intercepted until a scheduled payment is due to be made or sensitive information is due to be disclosed.

Intercepting emails

The most difficult phishing activities to detect occur where a large number of parties are copied in to email correspondence and where various irregular (one-off) payments are made. The greater the number of parties that are copied in, the greater the risk an email will be intercepted and a new, but similar, address inserted belonging to the fraudster.

Many Members maintain high levels of cyber-security and protect themselves from direct cyber-attacks. However, due to the international nature of the shipping industry and the varying cyber-security standards applied, fraudsters will commonly attack parties with the least secure systems to gain access to correspondence.

Arranging payments by email

Once the fraudster has been able to intercept messages, they may provide substitute bank account details at the last moment, using the correct account name but a different account number and sort code. It is common practice for banks not to check the name of the account holder to which payments are made. Rather, banks often just check the account number and sort code (IBAN) for payments. So, the fraudster can improperly use the name of the legitimate party meant to receive the funds, but have the payment made to their own bank account and sort code (IBAN). The party arranging the payment then believes they are paying the correct person until it is too late.

Avoiding the risk of fraud

The Association has encountered various phishing attempts and procedures are in place to detect and counteract these challenges, including :

1. Making sure our email system is as secure as possible, including the use of strong passwords and anti-phishing software.

2. Limiting the number of parties in correspondence. Not only is this good practice given increasing data protection legislation (e.g. GDPR in the EU), it helps to minimise sensitive correspondence being seen unnecessarily by parties who have no genuine involvement in the correspondence. This is particularly important when corresponding on details of proposed payments or a change of bank accounts.

3. When providing settlement or banking details, avoiding 'reply all' and, instead, consider typing email addresses or checking email addresses from the recipient's website or company stationary. Verifying email addresses reduces the opportunity for the fraudsters being aware of when payments are to be made.

4. When a third party informs of a change in their bank account details or provides new account details for the first time, cross checking by alternative means of communication to verify the new bank account details (again using previously verified contact detail and not those provided in the request to change the payment details).

5. Raising awareness of the risk of phishing and encouraging employees to routinely check the email addresses used when sending or receiving emails and being alert to requests for changes of bank account details particularly when payments need to be arranged on an urgent basis.