Fraud - Business email compromise

Do you know the red flags to look out for?

If you work in the international supply chain, you are at risk of being unwittingly exposed to many types of payment fraud during the normal course of business.

What are the risks?

Which types of business email compromise are most common in my industry?

PAYMENT FRAUD

A fraudster pretends to be a business you make regular payments to, instructing you to make a payment to an alternative account. Often, the email address they use will be almost identical to your known contact.

CEO FRAUD

An email purporting to be from your CEO instructing you to urgently transfer funds to a new customer, using an email and details very similar to those you are already familiar with.

PROCUREMENT FRAUD

Fraudsters may pretend to be a previous subcontractor requesting an invoice be paid for their services. Often they will infiltrate computer systems and email traffic to gather information they need to make their claim believable.

WATCH OUT FOR RED FLAGS

- Instructions to make a payment into a new account
- An email address that is slightly different than usual
- Urgent and unusual payment instructions from senior staff members
- Invoiced goods/services that cannot be accounted for
- Lack of correlation between the invoice and your own records
- Payment requests that exceed total purchase order or agreed limits
- Ensure that all staff are educated to spot the signs and are aware of the procedures to follow should they suspect fraudulent activity
- Do not be intimidated by any perceived time pressure to act on instructions – take the time to ensure that the invoice is genuine
- Remember these simple rules if you have any suspicions about instructions: STOP, THINK, INVESTIGATE, CONTACT, REPORT

TT CLUB IS MANAGED BY **THOMAS MILLER**

STOP, THINK, INVESTIGATE, CONTACT, REPORT.

For more information: