COVID-19 - Increased risk of fraud during pandemic

Numerous scams have appeared during the coronavirus pandemic, which aim to exploit the increased volume of electronic communications arising from closed offices and isolated workers.

Members are reminded to exercise caution when opening and responding to emails, telephone calls and text messages during the coronavirus pandemic, and familiarise themselves with the current range of scams:

- Fake links via email to Microsoft Teams, Google Meet and Zoom meeting platforms
- Fake text messages for mobile phone-based contact-tracing applications
- Phishing emails purporting to be from your colleague, asking for personal details prior to return to work
- Phone calls from individuals posing as banks, HMRC or the Government, Department of Education, all offering services in return for bank or personal details
- Emails entitled 'you are infected' aimed to replicate the Government's own test and trace initiative, which may contain a Microsoft Excel document infected with malware
- Emails and texts advertising free or paid for Coronavirus testing kits for home or workforce. Note: Such a product does not currently exist.
- Fake text messages from the NHS or HMRC offering tax refunds

BALI urge members to verify information and requests for data with Government websites in the first instance, and exercise caution when making online purchases. Always scrutinise website addresses and emails from colleagues requesting the transfer of personal information, bank details or money. If in doubt, call colleagues on the telephone and verify the request directly with them.

Remember: It is easy for fraudsters to send and intercept emails from legitimate email accounts.