FRAUD RISK: Payroll Mandate Fraud

The Counter Fraud Team would like to make you aware of a type of fraud that targets organisations requesting for changes in bank details for staff. The team has already received two referrals from schools in Kent.

The fraud works by an email being sent from what appears to be a genuine employee's email account stating they have changed their bank details and requesting for them to be changed for the next pay run. The emails are sent directly from the fraudster to legitimate employees in the organisation that are responsible for this task.

The organisation will only become aware of the fraud on payday when the genuine member of staff does not receive their pay.

Social engineering techniques are used by fraudsters in order to obtain information on their targets.

It is important that your school has a robust process in place for staff who request a change to their bank accounts making sure that checks are carried out to verify the requests legitimacy.

DO:

- Verify changes in bank accounts with staff over the phone before any response is provided to the email.
- If you have online portals where these changes should be made direct staff to there, to minimise the fraud risk.
- If you receive a fraudulent request report it to internal.audit@kent.gov.uk, the Counter Fraud Team will submit a report to Action Fraud
- Mark the email as spam and delete

Don't:

- Reply to the email or engage with the criminal any further
- Feel pressured into making payment. You could be targeted again

For more information on types of frauds and how to prevent them please visit https://www.actionfraud.police.uk/

Invicta Audit and Counter Fraud

IACF Improving Outcomes Creating Value