Counter Fraud Team Alert: Phishing Emails sent to Schools

"Are you at your computer?"

The Counter Fraud Team have received reports from over 30 Kent Schools who have been targeted by fraudsters. Finance staff at the schools have received emails purporting to be a Senior Leader asking, "Are you at your computer?" staff replying to the email are receiving a response requesting for an Urgent Bacs/ Faster payment to be made. The email accounts sending the request are "spoofed" from the Senior Leaders making the emails look genuine.

This type of fraud is called Spear Phishing, whereby criminals specifically target senior members of staff in order to obtain financial or personal information.

What to look out for:

- If the sender has asked "Are you at your computer?".
- If you haven't responded, have they sent another email requesting a payment to be made?
- The sender's email address could appear very similar to a school's domain with minute differences in the email address.
- A sense of urgency; The email asks the member of staff their availability to make a payment.
- Payee details included in the email with a new supplier and bank account.
- The member of staff may receive an email asking for a sum of money to be paid into a bank account for a "new project" or for a "supplier".
- Spelling mistakes and/or incorrect grammar.

What to do:

- **Never respond to the email – This increases the risk you will be targeted again.**
- Be vigilant about emails from all sources that request payments.
- Pick up the phone and call the member of staff that has sent the request using the telephone number you hold, not the telephone number on the suspected email.
- Hover over the email address that sent the email, see if it changes from a genuine. email account that's not in your domain.
- Never respond to the email.
- Report the email to the Counter Fraud Team.
- Check with your IT department that your firewall software is up to date.
- Share this information with colleagues.
- Block the sender and delete the email.
- Create a specific email that is only used internally and has a "white list" of internal email addresses for finance to accept internal request for payments. This is not to be publicised externally. Please discuss this with your IT.

The Counter Fraud Team are reporting each referral to Action Fraud. Action Fraud have advised they are engaging with financial institutions to investigate the matter further so please keep referring incidents to us.

Contact Details:

If your school receives this type of email or you wish to seek advice, please contact:

Internal.audit@kent.gov.uk