**Department of Education Phishing Scam**

The National Fraud Intelligence Bureau has released an alert regarding a phishing and ransomware campaign currently in circulation which is targeting schools. The purpose of this scam is the distribution of ransomware through what appears to be a malicious email attachment.

Schools who have reported this scam advise that they have received a telephone call from an individual purporting to work to the Department of Education. This individual requests the email address of the Head Teacher or Financial Administrator claiming that guidance documents are to be sent containing sensitive information which cannot be forwarded to a generic school inbox.

When received, the email includes a zip file attachment, which could potentially be masked as an Excel or Word document. If downloaded, ransomware within the attachment will encrypt files and demand up to £8,000 to recover them.

Audit Services have recently received similar reports from Derbyshire schools who have been targeted by these fraudsters, however due to the diligence shown by these staff members, email addresses were not disclosed leading to the termination of the call by the caller with no further action taken.

It should be noted that similar scams have recently been reported whereby individuals have claimed to work for the Department for Work and Pensions and telecoms providers. In these cases the caller has requested to speak to the Head Teacher in connection to ‘internet systems’.

If staff receive such calls, Audit Services should be promptly notified and in the event that an email of unknown origin is received, it should be deleted immediately. Staff are reminded of the following when dealing with unexpected or suspicious emails;

 Do not open attachments;

 Do not click on embedded links within emails from unknown sources, instead roll the cursor over the link to reveal its true destination;

 Do not reply to unwanted emails;

 Do not forward suspicious emails.