Intelligence Alert UPDATE

GPMS: **OFFICIAL** ☐ **OFFICIAL-SENSITIVE** ☑

Evaluation		
Source Evaluation	**1**	**Reliable**
Intelligence Evaluation	**A**	**Known directly**
Handling Code	**C**	**Lawful sharing permitted**
National Intelligence Model Level	**2: Cross Border** **More than one LA member affected**	
Handling Conditions	**Cannot be shared outside of the member organisation with the exception of sharing with schools and academies, which must also follow handling instructions.** **Contents must not be uploaded to any public facing websites**	

Head Teacher Impersonation Fraud

NEW Mandate fraud appears to be trending at present, targeting schools or academies and seeking monies by purporting to be senior members of staff. A further member has reported an incident of Head Teacher Impersonation Fraud. On this occasion, only an initial email was sent to a member of staff at the school, which purported to be from the Head Teacher. Fortunately, the member of staff recognised that the email was fraudulent and took no action on it. The legitimate domain name for the school ends in **sch.uk.** The fraudulent email address was **chinedu10okoro@gmail.com.** A copy of the email received appears below. Note the wording in the email appears unusual for a Head Teacher to send to a member of staff and is in no way typical of correspondence at this school:-

From: <chinedu10okoro@gmail.com>
Date: 26 August 2021 at 09:00:17 BST
To: .sch.uk
Subject: Urgent Task

Hello

I have an urgent task for you to carry out as soon as possible. Hope you don't have so much at hand? if you do, I will need you to pend all for now.

Drop your WhatsApp number so I can send you a text and enlighten you about it all.

Thanks

Headteacher
School

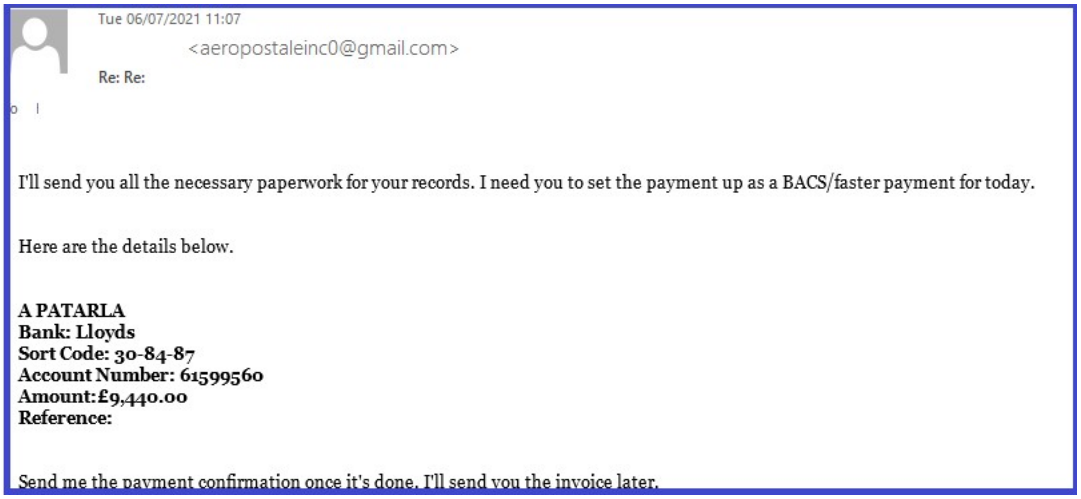
Head Teacher/Chief Executive Officer Impersonation Fraud

(Alert issued 27 August 2021)

We are advised the school received an email purporting to be from the Head Teacher. On this occasion the email was received by the School Office Manager, requesting a same day payment to discharge an invoice in the sum of £9,440. The legitimate domain name for the school ends in **sch.uk.** The fraudulent email address was **aeropostaleinc0@gmail.com**. The Bank details provided are below:-

Bank Account Name	Sort Code	Account Number
Lloyds	308487	61599560

An image of the email received appears below. Note the similarities in the wording of the email and layout of the banking details with the email image in our Alert issued 20 August 2021.*



Tue 06/07/2021 11:07

<aeropostaleinc0@gmail.com>

Re: Re:

I'll send you all the necessary paperwork for your records. I need you to set the payment up as a BACS/faster payment for today.

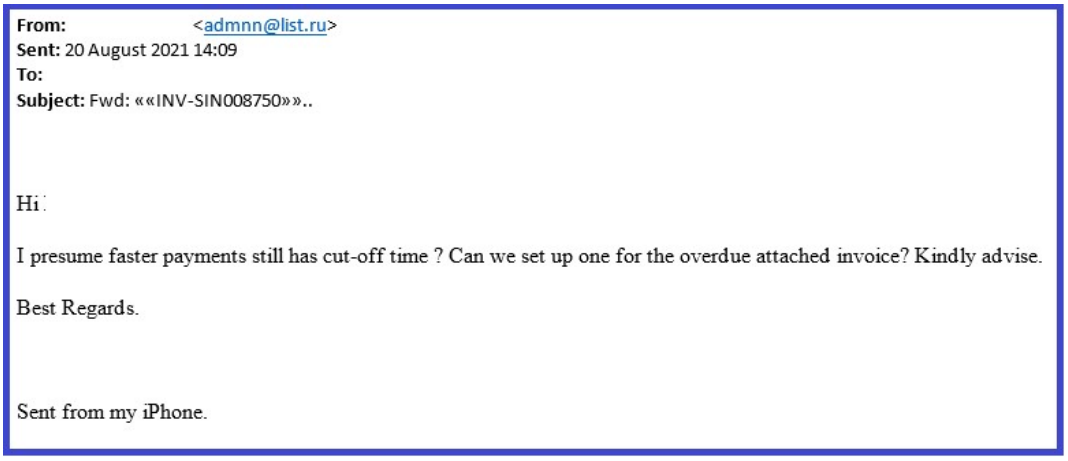
Here are the details below.

A PATARLA
Bank: Lloyds
Sort Code: 30-84-87
Account Number: 61599560
Amount:£9,440.00
Reference:

Send me the payment confirmation once it's done. I'll send you the invoice later.

Chief Executive Officer Impersonation

A member organisation reports an Academy Trust (which oversees three academies) received an email targeting the Trust Finance Director, allegedly from the Chief Executive Officer asking for a faster payment to be processed. The legitimate domain name for the Academy Trust ends in **trust.com**. The fraudulent email address used was **admnn@list.ru.** On this occasion, although the email referred to an invoice, there was no attachment to the email and no banking details were provided. A copy of the email appears below:



From: <admnn@list.ru>
Sent: 20 August 2021 14:09
To:
Subject: Fwd: ««INV-SIN008750»»..

Hi

I presume faster payments still has cut-off time ? Can we set up one for the overdue attached invoice? Kindly advise.

Best Regards.

Sent from my iPhone.

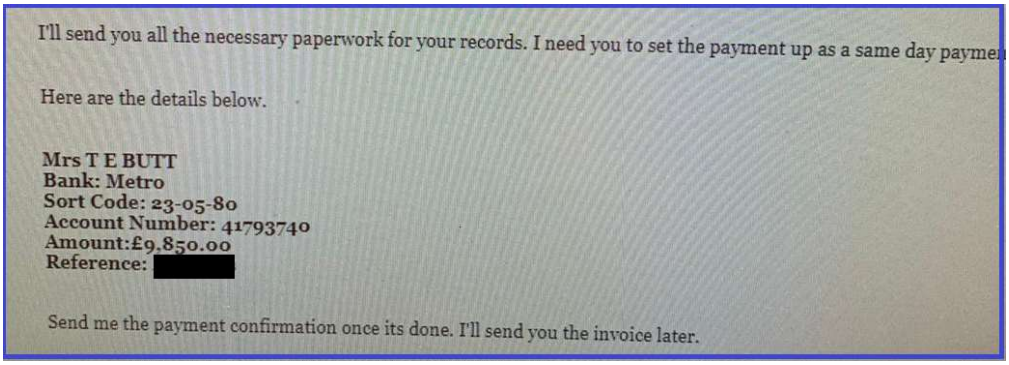
We have noted an increase in phishing emails and whaling attacks on schools in recent months and would urge all members to remind educational establishments in their areas to remain vigilant.

*Head Teacher Impersonation Fraud (Alert issued 20 August 2021)

A member authority has reported receipt of a phishing email by one of the schools in its area. An email was sent to the school's finance assistant; purporting to be from the Head Teacher; requesting that a same day payment be made to discharge an invoice in the sum of £9,850. The email advised the invoice would be provided, once payment confirmation had been received. This type of fraud relies on social engineering to manipulate the recipient to take action, given the level of seniority of the requesting individual. Although the email appeared to be from the Head Teacher's account, closer inspection revealed that the sending email address was not the Head Teacher's official email address. The domain name for the school ends in **sch.uk**. The fraudulent email address was **headteacher7054@gmail.com.** The banking details provided were:-

Bank Account Name	Sort Code	Account Number
Metro	230580	41793740

An extract from the email received appears below.


I'll send you all the necessary paperwork for your records. I need you to set the payment up as a same day payme

Here are the details below.

Mrs T E BUTT
Bank: Metro
Sort Code: 23-05-80
Account Number: 41793740
Amount:£9,850.00
Reference: [redacted]

Send me the payment confirmation once its done. I'll send you the invoice later.

We would ask members to remind their local educational establishments and businesses to continue to be vigilant when dealing with any emails requesting payments or changes to bank accounts, irrespective of who is requesting the change to be made.

If you would like to report any instances of the above information being used in similar fraud attempts please email them to intel@nafn.gov.uk and the details will be forwarded to the relevant teams. Please also report to Action Fraud.

Alerts provide information about fraud, risks and trends which may affect members; your contributions are vital – please email them to NAFN. Where appropriate please include handling restrictions.