Intelligence Alert

GSC OFFICIAL ☐ OFFICIAL-SENSITIVE ☑

Evaluation		
Source Evaluation	1	Reliable
Intelligence Evaluation	A	Known directly
Handling Code	C	Lawful sharing permitted with conditions
National Intelligence Model Level	2: Cross border More than one member affected	
Handling Conditions	Cannot be shared outside of the member organization (except Schools). Contents must not be uploaded to any public facing websites	

School Mandate Fraud Alert

Outlook Account Compromise

A NAFN member reports that a school in their partnership has been targeted in a sophisticated mandate fraud, which was enabled by an Outlook account compromise. It is believed the account compromise occurred on or around September 2023 and targeted the Head Teacher of the school.

Between September 2023 and February 2024, several rules were set up on the Head Teacher's Outlook account without their knowledge. The rules diverted emails to subfolders which referenced invoices or were from specified staff. As the mandate fraud was executed five months after the original compromise, it is possible the fraudsters monitored the account before setting up the rules, as only emails from relevant staff responsible for invoices/accounts payable were identified.

In February 2024, emails from a supplier submitting invoices for payment were intercepted. As a result of the compromised account and rules, the invoices were not seen by the true account holder and the fraudster was able to alter the invoice and change the bank account details. The falsified invoice was then sent from the Outlook account to the treasurer of the bank account approving payment. The fraud was only identified when the supplier chased payment from the school. The account details provided by the fraudster are below and the bank confirms the account is now closed:

Bank Name: PAYONEER
Sort Code: 23-14-86 Account Number: 15184785

Following the identification of this fraud, a further school has confirmed experiencing a similar occurrence involving a compromised outlook account and rules designed to monitor the administration of invoices/payments. Please share with schools and accounts payable to identify if payments have been made to this fraudulent account.

NAFN receive many reports of Mandate Fraud but given the potential loss to the public purse, it is important to continue raising awareness. Please distribute this alert among relevant staff members. **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.