National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

'Department of Education' Phishing Scam Phishing and Ransomware Alert

December 2016

‘Exam Guidelines Phishing Campaign and RansomwareAlert

The information contained within this alert is based on numerous reports to Action Fraud and other sources. The purpose of this alert is to increase awareness of the phishing campaign currently in circulation. The campaign’s primary function appears to be distributing ransomware, through an email attachment believed to be malicious.

The alert is aimed at schools, local police forces, governmental agencies and members of the public.

ALERT

Fraudsters are initially calling education establishments claiming to be from the Department of Education. They then ask to be given the personal email and/or phone number of the head teacher/financial administrator. The fraudsters claim that they need to send guidance forms to the head teacher (these so far have varied from exam guidance to mental health assessments). The scammers on the phone will claim that they need to send these documents directly to the head teacher and not to a generic school inbox, using the argument that they contain sensitive information.

The emails will include an attachment - a .zip file (potentially masked as an Excel or Word document). This attachment will contain ransomware, that once downloaded will encrypt files and demand money (up to £8000) to recover the files.

It should be noted that similar scam attempts have been made recently by fraudsters claiming to be from the Department for Work and Pensions and telecoms providers (in this case they need to speak to the head teacher about ‘internet systems’).

PROTECTION / PREVENTION ADVICE

Having up-to-date virus protection is essential; however it will not always prevent you from becoming infected.

Please consider the following actions:

- Although the scammers may know personal details about the head teacher and use these to convince you they are a real employee, be mindful of where these have been obtained from, are these listed on your public facing website?
- Please note that the “Department of Education” is not a real government department (the real name is the “Department for Education”).
- Don’t click on links or open any attachments you receive in unsolicited emails or SMS messages. Remember that fraudsters can ‘spoof’ an email address to make it look like one used by someone you trust. If you are unsure, check the email header to identify the true source of communication.
- Always install software updates as soon as they become available. Whether you are updating the operating system or an application, the update will often include fixes for critical security vulnerabilities.
- Create regular backups of your important files to an external hard drive, memory stick or online storage provider. It’s important that the device you back up to aren’t left connected to your computer as any malware infection could spread to that too.

- Do not pay extortion demands as this only feeds into criminals' hands, and there's no guarantee that access to your files will be restored if you do pay.
- If you think your bank details have been compromised, you should immediately contact your bank**.**
- If you have been affected by this, or any other scam, report it to Action Fraud by calling **0300 123 2040**, or visiting www.actionfraud.police.uk.

FEEDBACK

The NFIB needs feedback from our readers to evaluate the quality of our products and to inform our priorities. Please would you complete the following NFIB feedback survey through: https://www.surveymonkey.com/r/FeedbackSDU. This should take you no more than 2 minutes to complete. If you have other feedback or additional information that you would prefer to provide by email please send to NFIBfeedback@cityoflondon.pnn.police.uk.

Handling Instructions

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared, other than with the agreed readership/handling code, without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998.

The cover sheets must not be detached from the report to which they refer.

Protective Marking:	**Not Protectively Marked**
FOIA Exemption:	NO
Suitable for Publication Scheme:	NO
Version and Date:	V1
Storage File Location:	G:\OPERATIONAL\Fraud_Intel\Cyber Crime Desk\Alerts
Purpose:	Department of Education phishing scam
Owner:	NFIB Cyber
Author:	105098P
Reviewed By:	DI MACE