National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

PBX/Dial-Through Fraud Threat to Schools

July 2016

PBX/DIAL-THROUGH FRAUD THREAT TO SCHOOLS

The purpose of this alert is to provide knowledge and prevention advice to help schools protect themselves from PBX and dial through fraud.

The NFIB has seen a significant rise in the number of reports made in relation to this type of fraud. Around 6% of the total of these reports relate to a school or college, although this is only based on what is reported and the figure could be much higher.

The losses involved can be high, especially when they are made during times that a school may be closed, for example the summer holidays. During this period it is likely that the fraudulent calls will go un-noticed until the telephone bill arrives. Since 2012 Action fraud has recorded the total losses to schools to be £186,923.09; an average loss of £1,683 per school.

ALERT CONTENT

What is PBX Fraud?

Private Branch Exchange (PBX) is a telephone switching system that connects internal telephones, as well as connecting them to the Public Switched Telephone Network (PSTN), Voice over Internet Protocol (VoIP) providers and Session Initiation Protocol (SIP) Trunks. The PBX will often allow access to voice messaging systems.

PBX/dial-through fraud occurs when hackers target these systems from the outside and use them to make a high volume of calls to premium rate or overseas numbers to generate a financial return.

How does it work?

Depending on the type of system used there are a number of ways a hacker may gain access to a traditional or IP based PBX system, whether internal to the company or through a hosted service.

Incorrectly configured firewalls and set ups, poor security settings, lack of maintenance as well as the use of default/easy passwords allow quick and easy access for the hackers.

Once access is gained, the criminals can exploit in-built services such as voicemail, call forwarding and call diversion to direct calls to a number of their choosing. This will often be to premium rate or international numbers.

In this fraud the criminal tends to make their money in two ways:

i. Dialling premium rate numbers that are associated with international calling companies.
ii. Dialling international numbers through the compromised telephone system, most noticeably to Eastern Europe, Cuba and Africa.

In both instances the suspects will either have a share in the revenue generated by the calls or they will be paid for their hacking services in advance.

This type of fraud is most likely to occur when organisations are most vulnerable i.e. during times when businesses are closed but their telephone systems are NOT; for example in the early hours of the morning or over a weekend or public holiday.

PROTECTION / PREVENTION ADVICE

Protect:

The good news is that some simple steps will significantly reduce your risk of becoming a victim:

- If you still have your voicemail on a default PIN/password change it immediately.
- Use strong PIN/passwords for your voicemail system, ensuring they are changed regularly.
- Disable access to your voicemail system from outside lines. This is usually used for remote workers to access. If this is not business critical then disable it or ensure the access is restricted to essential users and they regularly update their PIN/passwords.
- If you do not need to call international numbers/premium rate numbers, ask your telecoms provider to place a restriction on your telephone line.
- Consider asking your network provider to not permit outbound calls at certain times e.g. when your business is closed.
- Ask your telecoms provider to alert you immediately if there is any unusual call activity taking place on your telephone lines.
- Ensure you regularly review available call logging and call reporting options, regularly monitor for increased or suspect call traffic.
- Secure your exchange and communications system, use a strong PBX firewall and if you don't need the function, close it down.
- If you use a maintenance provider speak to them or ensure that the person responsible for the PBX understands the threats and ask them to correct any identified security defects.
- Consider consulting an IT telecoms professional to ensure your settings for your PBX systems are secure and the settings have been properly set up.

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:	Yes
Version:	V1.0
Storage File Location:	NFIB
Purpose:	Fraud Alert
Owner:	NFIB Management
Author:	100735G
Review By:	Senior Analyst 88071e