Article by Ian Buss. Head of Education. Lloyds Bank

Social Engineering – Increasing Fraud Threat

Lloyds Banking Group, Commercial Banking, Fraud Risk Management team have experienced a three-fold increase in social engineering driven fraud attempts being reported by schools during 2017. These attacks are operated by fraud groups targeting staff within schools, with some sort of confidence trick designed to dupe the victim into making a payment, redirecting a legitimate payment to an account under the fraudster's control, releasing PIN or card/reader credentials or to move funds to allegedly 'safe' accounts.

The key fraud attacks are:-

- CEO Fraud
- Invoice Fraud
- Vishing

Whilst 3 out of 4 attempts reported to the Bank by schools are prevented either due to good awareness by the school employees or bank controls, it is vital that schools remain vigilant to the threat and implement effective controls to identify and prevent these attacks.

Summary of Attack Methods

CEO Fraud

Instruction purporting to have originated from a senior official requesting an urgent payment to a specified bank account. These instructions commonly replicate language, terms and phrases regularly used by the supposed sender and are sent at a time when the recipient is likely to be under pressure e.g. month end and at a time when the sender is not available for contact.

Invoice Fraud

Redirection of a payment to a genuine supplier/contractor. An instruction is received advising of a change of bank account or a forged invoice which appears to be from a regular supplier/contractor requesting payment to a nominated account.

Vishing (Telephone Scam)

Call purporting to originate from a trusted source, often allegedly from the Bank's Fraud Dept. The intention is to trick the call recipient into taking action under the misapprehension that it is required to protect the school's money. This could be to download software allowing the attacker to take remote control of the computer, or to disclose passwords/card – reader codes to allow the attacker to set up fraudulent payments, or to trick the victim into moving money to accounts described as safe/secure.

Critical Actions to Prevent These Attacks

CEO Fraud

- Have a process in place to ensure that all payment instructions are confirmed regardless of whether the instructions says it's 'urgent' and/or 'strictly confidential'. Refer to the sender or someone else in authority if the sender is unavailable
- Do not rely on the email address appearing to be legitimate or the wording to be familiar

Invoice Fraud

- Authenticate any instruction to change details of a supplier/contractor, particularly if the notification is a change of beneficiary bank account number. Call the supplier/contractor on a number independently sourced e.g. supplier's website
- Have a process in place to validate that invoice requests are legitimate

Vishing

- Authenticate a call by calling the organisation back on an independently sourced number e.g. bank website
- Never rely on the number appearing on your caller display as confirmation of the source of the call. These numbers are easy to spoof
- Remind all staff that banks will never call to ask for full passwords, PIN's, card/reader codes.
- Have dual authorisation set with your online banking provider to set up new payment instructions
- Only download software from sources you trust. Be highly cautious if asked to download software from a caller that you've not authenticated

General Advice

- Raise awareness of these fraud attack methods with all staff
- Review your processes to ensure staff are able to confirm unusual instructions and they know what to do
- Provide fraud risk training and refresh on a regular basis
- Speak to your bank manager on a regular basis to keep abreast of the latest fraud trends
- If you do identify that a fraudulent payment has been made, let your bank know immediately

Information on these and other fraud scams can be found by visiting www.lloydsbank.com/fraud or www.bankofscotland.co.uk/fraud

Schools are also recommended to encourage their staff to visit the 'Take Five' website - www.takefive-stopfraud.org.uk/ which offers practical advice to avoid falling victim to the most common, social engineering driven fraud attacks. The Take Five campaign is led by UK Finance, funded by the banking industry and backed by the UK Government.